INSTITUTO POLITÉCNICO DE BEJA

ESCOLA SUPERIOR DE TECNOLOGIA E GESTÃO

Curso de Mestrado em Engenharia de Segurança Informática

Governance Enterprise of Information Technology

Garantia da Informação na Administração Local

Pedro Miguel Caetano Mendes dos Santos

Beja

2014

INSTITUTO POLITÉCNICO DE BEJA

ESCOLA SUPERIOR DE TECNOLOGIA E GESTÃO

Curso de Mestrado em Engenharia de Segurança Informática

Governance Enterprise of Information Technology

Garantia da Informação na Administração Local

Dissertação de mestrado apresentado na Escola Superior de Tecnologia e Gestão do Politécnico de Beja

Elaborado por:

Pedro Miguel Caetano Mendes dos Santos

Orientado por:

Doutora Isabel Sofia Sousa Brito

Beja

2014

Resumo

Esta dissertação pretende propor uma EGTIC (Estrutura de Governação para as Tecnologias de Informação e Comunicação) no âmbito da garantia e segurança da informação, associada especificamente à administração local. Esta proposta assenta nas boas práticas existentes a nível mundial no que diz respeito à governação e gestão das TI (Tecnologias de Informação) e segurança nos sistemas de informação, pois pretende-se identificar o posicionamento das TIC na organização. Assim pretende-se o reconhecimento das TIC como parceiros de negócio e fonte de criação de valor, ao invés de unicamente fonte de suporte ao mesmo negócio. Este reconhecimento terá como consequência a integração da governação das TIC na governação do município.

A proposta para a implementação da EGTIC no município é baseada no guia de implementação do CobiT 5. Este guia também orienta o programa de implementação e a forma de concretizar cada uma das fases do ciclo de melhoria contínuo, incluindo a forma de utilizar outras ferramentas tais como o ITIL ou a ISO/IEC 27000.

É apresentado um caso de estudo usando o *Appendix D. Example Business Case* do guia de implementação do CobiT 5, assim como, as matrizes fornecidas pelo mesmo guia e pelo próprio *Framework.* A sua aplicação permitiu chegar a algumas conclusões, tais como, i) a morosidade de cada interação do programa; ii) a necessidade da mitigação de alguns riscos, como por exemplo, o necessário apoio do executivo; iii) a identificação de atividades relevantes na área da segurança e garantia da informação; iv) a segurança da informação é salvaguardada ao nível do **risco assumido**, garantindo-se a **otimização dos recursos** com a priorização (pela EGTIC) baseada em justificações estratégicas; v) a criação do desejo de agir perante os resultados da análise de capacidade do município/processos.

Abstract

The aim of this dissertation is to propose an GEITS (Governance Information Technologies Structure) in the context of information assurance and security specifically associated with local government.

This proposal is based on global best practices with regard to the governance and management of ITs (Information Technologies) and security in the information systems since its aim is to identify the position of the ICTs within the organisation. Thus, appreciating ICTs as business partners and a source of value creation rather than purely as a source of support to the business itself is the intention. The effect of this appreciation will be the integration of ICT governance into the governance of the municipality.

The proposal for implementing the GEITS in the municipality is based on the CobiT 5 implementation guide. This guide also directs the implementation programme and the method for incorporating each phase of the continuous improvement process, including how to use other tools such as ITIL or ISO/IEC 27000.

A case study of its use appears in Appendix D. Example Business Case of the CobiT 5 implementation guide as well as the blueprints provided by the guide and the framework itself. Its application entailed certain conclusions such as i) the length programme's interaction time; ii) the need to mitigate some risks, for example, the need of executive support; iii) the identification of relevant activities in the field of information security and assurance; iv) the security of the information is guaranteed according to the risk assumed thereby ensuring optimised resources with prioritisation (through the GEITS) based on business cases; v) the desire to act created when faced with the results of the municipality/processes capacity analysis.

Agradecimentos

Gostaria de deixar aqui expresso os meus mais sinceros agradecimentos à minha orientadora Doutora Isabel Sofia Sousa Brito, pois se não fosse ela, garantidamente não teria força e incentivo para neste momento estar pronta.

À minha família um agradecimento especial pelo incentivo e força proporcionados quando demonstrei pela primeira vez a intenção de obter os conhecimentos que este mestrado me proporcionou.

A todos os meus colegas de mestrado que comigo trilharam os caminhos da engenharia de segurança informática, com um especial abraço de agradecimento ao Eng. Filipe Vieira e Eng. Rui Pereira, também eles finalistas deste grau.

Para terminar, aos meus colegas de trabalho, em especial ao Eng. Melo Pereira que sempre proporcionou com os seus conhecimentos na área todo o apoio solicitado, assim como ao Dr. Humberto Chula por se ter juntado tão afincadamente ao projeto e participado na aplicação prática do mesmo.

Índice

(Todos os Anexos e Apêndices só em suporte Digital)

Índice de Figuras

Índice de Tabelas

Lista de Acrónimos

É apresentado de seguida uma lista com os acrónimos utilizados ao longo desta dissertação, julga-se que assim poder-se-á simplificar a leitura.

APDSI	Associação para a promoção e desenvolvimento da sociedade da informação;
BC	Continuidade no Negócio;
BMIS	*Business Model for Information Security*;
BSI	*British Standards Institution*;
C&A	Certificação e Acreditação;
CCSC	*Commercial Computer Security Centre*;
CCTA	*Central Computer and Telecommunications Agency*;
CIO	*Chief Information Officer*;
CMDB	*Configuration Management Database*;
CMMI	*Capability Maturity Model – Integration*;
CMP	Câmara Municipal de Portimão;
CobiT	*Control Objectives for Information and related Technology*;
COSO	*Committee of Sponsoring Organizations of the Treadway Commission*;
CRM	*Customer Relationship Management*;
DMSI	Divisão de Modernização e Sistemas de Informação;
EGTIC	Estrutura de Governação das Tecnologias de Informação e Comunicação;
ERP	*Enterprise Resource Planning*;
DSRM	*Design Science Research Methodology*;
DR	Recuperação de Desastres;
IA	*Information Assurance*;
IS	*Information Security*;
ISO/IEC	*International Organization for Standardization/International Electrotechnical Commission*;

ITAF	IT Assurance Framework;
ITIL	*Information Technology Infrastructure Library*;
itSMF	*The IT Service Management Forum*;
KPI	*Key Performance Indicator*;
PDCA	*Plan-Do-Check-Act*;
PGERRTIC	Plano para a Racionalização e Redução de Custos nas TIC, na Administração Pública;
OGC	*Office of Government Commerce*;
SGSI	Sistema de Gestão da Segurança da Informação;
SI	Sistemas de Informação;
SLA	*Service Level Agreement*;
TIC	Tecnologias de Informação e Comunicação;
TOGAF	*The Open Group Architecture Framework*;
UO	Unidade Orgânica;
Val IT	*Value IT Framework*;

1.Introdução

O objetivo deste capítulo é o de contextualizar a governação das TIC na administração pública e em particular na administração local, identificar o problema da governação das TIC, no que diz respeito à garantia da informação, abordando o paradigma de *Information Security* versus *Information Assurance,* e porque deve ser resolvido. Face a este problema, é presentada uma solução, e os seus objetivos, que passam pela implementação de uma EGTIC.

1.1. Contextualização

Para ajudar a contextualizar, seguem algumas definições de governação de TIC:

"*The set of processes that ensure the effective and efficient use of IT in enabling an organization to achieve its goals*." © 2010 Gartner, Inc. All rights reserved. [1]

"*A decision-making framework for IT investments that is designed to maximize the return of benefits while managing risk to acceptable levels*." © 2010 Forrester Research, Inc. All rights reserved. [2]

"*Specifying the decision rights and accountability framework to encourage desirable behavior in using IT*" © Peter Weill & Jeanne W. Ross (MIT CISR) All rights reserved. [3]

1.1.1. O que é a Governação para as Tecnologias de Informação e Comunicação

O atual contexto económico-social, nomeadamente os desafios económicos e financeiros, promove alterações profundas na forma de exercer a governação na administração pública local. Estas colocam em foco a necessidade de maiores níveis de eficácia, mais garantia e maior transparência na informação e tudo a um menor custo, em toda a estrutura municipal e em particular, na área das TIC.

Uma visão para alavancar as TIC no sentido de aumentar a eficiência do município, exige uma capacidade de supervisão ou governação das mesmas que garantam a participação igual e adequada, de todas as áreas que compõem a estrutura do município, no processo de tomada de decisão relativo aos investimentos nas TIC.

A GTIC (Governação das Tecnologias de Informação e Comunicação) assegura que i) as necessidades, condições e opções das partes interessadas, são avaliadas na determinação dos objetivos a ser alcançados pela organização; ii) a definição da orientação através da priorização e de um processo de tomada de decisão; e iii) a monitorização do desempenho e conformidade dos objetivos e orientação previamente acordados.

As funções normalmente atribuídas à UO (Unidade Orgânica) responsável pelos SI (Sistemas de Informação) e pelas TIC são de algum modo originais quando comparadas às de outras UO nos municípios. Englobam muitas atividades relacionadas com a tecnologia que, por vezes, mais se assemelham a atividades de investigação e desenvolvimento, do que a atividades processuais ou legais como acontece em outras UO. As UO responsáveis pelas TIC e SI são criadas para fornecer serviços baseados em tecnologia a todos os elementos da jurisdição em que opera.

Uma vez que é orientada aos serviços, esta UO deve receber um *feedback* contínuo dos utilizadores dos seus serviços quanto à sua orientação e desempenho.

Devido à sua natureza técnica, a prestação de serviços na área das TIC requer métodos de controlo únicos, que normalmente não são aplicáveis a outras áreas do município. Esse controlo deve garantir que são servidos os melhores interesses do município e, ao mesmo tempo, assegurar que os serviços prestados aos munícipes e utilizadores dos sistemas são relevantes, assertivos e de baixo custo. Esta forma de controlo é melhor aplicada através da utilização de uma EGTIC.

1.1.2. Qual a importância de uma estrutura de suporte à GTIC

De um modo geral, quer no sector público quer no privado, existe um reconhecimento crescente de que a informação é um recurso chave, e que as TIC são ativos estratégicos que dão um contributo importante para o sucesso das organizações. A verdade é que as TIC são um recurso poderoso que podem ajudar um município a alcançar os seus objetivos mais importantes. É nelas que se podem encontrar soluções de automatização de processos chave e podem ser elas também a base para novas estratégias, permitindo a redução de custos e a inovação na oferta de serviços digitais. As TIC poderão ainda ser utilizadas como ferramenta de aproximação ao munícipe através da recolha e tratamento de dados provenientes dos diversos sistemas, conseguindo assim fornecer uma visão de 360º do munícipe na sua relação com o município. [4]

São também a fundação da economia em rede que elimina barreiras geográficas e silos organizacionais, proporcionando novas e inovadoras formas de gerar valor. Por isso muitas organizações reconhecem que a informação e o uso das TIC são uma área crítica e estratégica que necessita de ser governada de forma apropriada. [4]

Enquanto as TIC têm o potencial para a transformação dos processos numa organização, muitas vezes também representam um investimento significativo. Frequentemente, grande parte dos gastos resultam da manutenção dos sistemas pós implementação e de custos operacionais ("no manter da máquina a funcionar"), em oposição a iniciativas de transformação ou inovação.

Muitas organizações ainda não conseguem demonstrar que os seus investimentos em TIC conseguiram acrescentar valor concreto e mensurável, concentrando-se agora numa EGTIC como mecanismo para resolver esta situação. [4] Além disso, a economia em rede apresenta uma série de riscos relacionados com as TIC tais como a indisponibilidade de sistemas, a divulgação de dados pessoais ou proprietários, ou

a dificuldade no desenvolvimento de soluções inovadoras devido a uma arquitetura dos sistemas de informação inflexível. A necessidade de gerir este tipo de risco é outra impulsionadora para uma melhor GTIC. [4]

Por último, a importância da EGTIC também pode ser atribuída aos complexos ambientes legislativos e reguladores que as organizações enfrentam hoje em dia, que impõem um maior e melhor controlo das operações. Uma EGTIC pode permitir que os complexos requisitos de conformidade[1] sejam alcançados de uma forma mais eficaz e eficiente. [4]

1.2. O Problema

Essencialmente o problema encontra-se no paradigma de IS (*Information Security*) versus IA (*Information Assurance*), complementaridade de ambos ou inclusão de um no outro, inserido num paradigma ainda maior que é o das TIC como serviço de suporte versus TIC como parceiro de negócio.

Para enquadrar a problemática convém ver algumas definições:

Information Assurance: "*Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. SOURCE: SP 800-59; CNSSI-4009* " [5]

Information Security: *"The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability. (Source: SP 800-37; SP 800-53; SP 800-53A; SP 800-18; SP 800- 60; CNSSI-4009; FIPS 200; FIPS 199; 44 U.S.C., Sec. 3542)*

Protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide—

1. *Integrity, which means guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity;*

[1] Estar conforme à legislação e demais regulamentos em vigor

2. *Confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and*

3. *Availability, which means ensuring timely and reliable access to and use of information. (SOURCE: SP 800-66; 44 U.S.C., Sec 3541)"* [5]

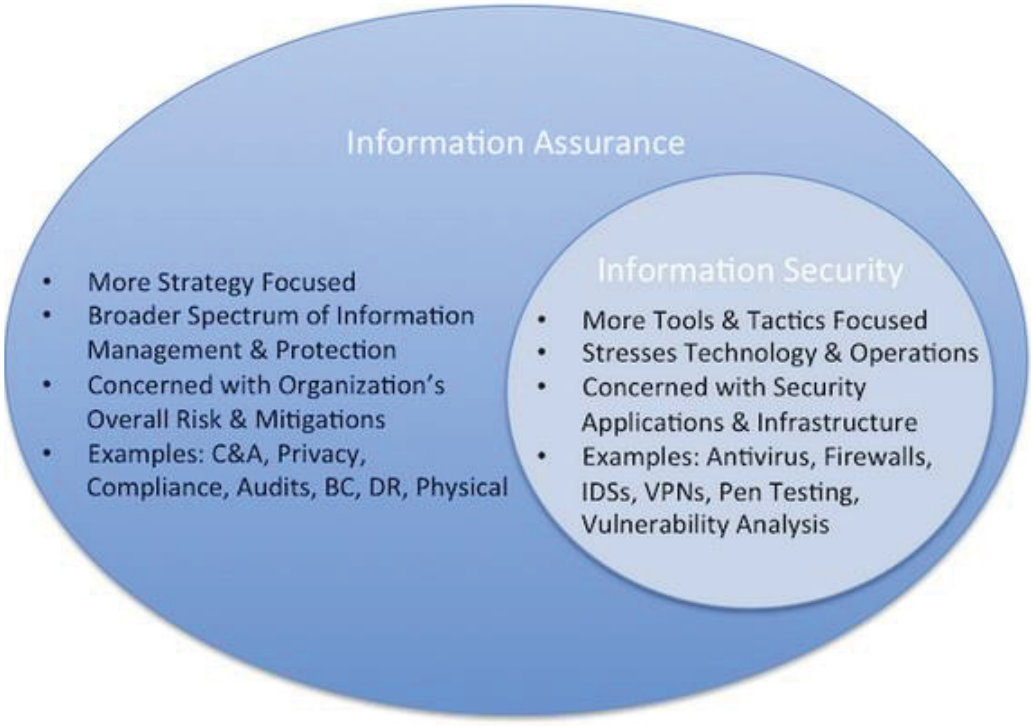


Figura 1 - Complementaridade de IA e IS obtido de [6]

No sítio web Nova Infosec[2] é possível encontrar um resumo interessante do que se pretende de cada uma das áreas IA e IS, concluindo que IS é uma componente da IA conforme se pode constatar da análise da Figura 1.

O problema tem origem no posicionamento das TIC na organização. A questão das TIC como parceira de negócios ao invés de unicamente prestadora de serviços de suporte, advém da necessidade de aliar a modernização de forma segura dos serviços com a emergente imposição de contenção de custos. Ao invés de se propor a utilização de meios tecnológicos que suportem processos não modernizados, pretende-se o alinhamento estratégico da missão e visão da organização, com aquilo que as TIC poderão garantir numa mudança de paradigma na entrega de serviços, neste caso ao munícipe. Este alinhamento é visto como as TIC a "trabalhar" de um modo governado. Acredita-se que a garantia de informação (do inglês *Information*

[2] https://www.novainfosec.com *WebSite* com informação para profissionais de segurança

Assurance) através das TIC a trabalhar de um modo governado e no interesse das partes interessadas não só alinhadas com a estratégia da organização, mas fazendo parte desta, será a melhor forma de se garantir uma informação segura sem desperdício de meios e fundos. Assim, podemos afirmar que a garantia da informação também deve fazer parte da estratégia da organização.

"Information Technology (IT) governance is important in every Enterprise to ensure the execution of the firm's security policies and procedures." [7]
"Information system security management goals can only be achieved if the policies and procedures are complete, accurate, available, and ultimately executed or put into action. Organizations must be conscious of the hazards associated with the diffusion of technology throughout the firm and must reflect this awareness through the purposeful creation of policy. The goals of IT security are to ensure the confidentiality, integrity and the availability of data within a system. The data should be accurate and available to the appropriate people, when they need it, and in the appropriate condition. Perfect security is not feasible — instead IT security managers strive to provide a level of assurance consistent with the value of the data they are asked to protect. It is within their structures and governance procedures that organizations are able to solve the issues of responsibility, accountability, and coordination toward the achievement of their purpose and goals." [7]

Neste sentido, diversas organizações, privadas e públicas, têm procurado seguir normas e *frameworks* para alinhar as atividades TIC com a missão e visão da organização, promovendo assim a governação das TIC tendo em vista uma gestão otimizada da segurança dos sistemas de informação.

1.3. Objetivos

Face aos problemas referidos na seção anterior, o objetivo desta dissertação é dar os primeiros passos para a implementação de uma EGTIC para a administração pública local promovendo a governação das TIC e consequentemente garantindo a informação e a sua segurança. Esta estrutura deve ser vista como parte integrante da governação municipal, capaz de exercer a supervisão adequada no planeamento, aquisição e implementação segura das TIC. Ela permitirá ao município tirar pleno partido das TIC, maximizando os benefícios, capitalizando as oportunidades e obtendo melhorias operacionais com a garantia da informação realmente relevante.

A EGTIC define como o planeamento, o investimento e as decisões de priorização são realizados e quem as realiza. Estabelece também a estrutura de responsabilização necessária para encorajar um comportamento desejável na utilização das TIC, nomeadamente aqueles comportamentos que são necessários para gerar o valor

cobiçável dos investimentos em TIC da forma mais segura dentro da criticidade determinada para os mesmos.

Fundamentalmente, a proposta de EGTIC preocupa-se com o valor criado pelas TIC para a organização e com a mitigação do risco que lhe está associado. Tal é possibilitado pela disponibilidade e por uma gestão dos recursos adequada, pela medição do desempenho e monitorização dos progressos na direção dos objetivos desejados.

Assim, são definidos para as EGTIC os seguintes objetivos [8]:

- Concretização de benefícios:
    - Criar valor público para as partes interessadas através das TIC:

      Os princípios básicos para criação de valor com as TIC são o fornecimento de serviços e soluções adequadas ao fim a que se destinam, em tempo útil e dentro do orçamento, tentando gerar os benefícios financeiros e não financeiros pretendidos. A descrição de valor público deve orientar-se pelos tipos de impacto que as TIC podem ter nos interesses das partes: financeiro, político, social, estratégico, ideológico e na administração do bem público. Deste ponto de vista resultam dois tipos de valor de igual importância: o valor que é criado diretamente para os cidadãos e empresas e o valor que é acrescentado à governação como bem público. Para cada um destes tipos de valor existem três mecanismos de geração de valor: aumentos de eficiência e/ou eficácia, facilitadores de atividades desejáveis que de outro modo seriam inviáveis, e melhorias intrínsecas para as partes interessadas, tais como a melhoria na transparência. [9]

    - Manter e criar valor com os investimentos já realizados;
    - Eliminar iniciativas e ativos que não estejam a criar valor suficiente;
    - Transparência na demonstração de impacto das TIC no município.
- Otimização do risco:
    - Enfrentar o risco associado à utilização, posse, operacionalidade, envolvimento, influência e adoção das TIC no município;
    - De eventos que potencialmente influenciem o município;
    - Preservação do valor criado;
    - Integração com a gestão de risco do município;
    - Influência do impacto da otimização do risco das TIC.
- Otimização de Recursos:

- Garantir os recursos e a capacidade de execução do plano estratégico;
- Providenciar uma infraestrutura de TIC económica e integrada;
- Integração de novas tecnologias e abate ou atualização de tecnologias obsoletas;
- Reconhecimento da importância das pessoas nos procedimentos para além do *software* e do *hardware*;
- Incidência na formação;
- Promover a retenção e garantia de competências chave do pessoal das TIC.

As TIC estão atualmente integradas no funcionamento dos serviços municipais, podendo ser consideradas nucleares à sua operação. A EGTIC, como estrutura de supervisão, será parte integrante da governação do município, e estará focada no desempenho das TIC e numa gestão eficaz do risco atribuível à dependência que a organização possui destas.

O executivo e a direção, assistidos por comissões de risco e auditoria, deverão garantir que o desempenho da EGTIC é avaliado, monitorizado, relatado e divulgado. A divulgação será baseada em relatórios obtidos das equipas de risco, conformidade, e de auditoria interna.

Assim, o objetivo último da governação é a criação de valor através da realização de benefícios e a otimização do risco e recursos. Por outro lado, se forem aplicados controlos de segurança a ativos de informação de forma não otimizada, podemos afirmar que estes até poderão estar seguros, mas não podemos afirmar que estão de forma otimizada o que não garante o valor desejável dos mesmos. Pretendendo-se assim que seja prestada informação relevante e confiável, às partes interessadas, sobre a qualidade do desempenho da EGTIC na garantia da informação.

Para este fim, a implementação de uma EGTIC, considera-se a doutrina do conhecido e reconhecido, adotando na medida do possível normas e *frameworks* existentes para a área, acrescentando assim uma mais-valia para a capacitação dos processos TIC governativos e não só, apoiada nos ciclos contínuos de melhoria.

1.4. Metodologia de investigação

Qualquer dissertação necessita de seguir uma filosofia por forma a fornecer a quem a lê a perspetiva de como esta deve ser interpretada. Assim pretende-se que a análise da mesma seja de fácil perceção e entendimento por quem o for fazer, permitindo que estas já se encontrem cientes do que irão encontrar, incluindo o âmbito e possíveis limitações.

Esta dissertação envolve maioritariamente sistemas de informação, o que também significa o envolvimento de pessoas, de uma ou outra forma. O foco da dissertação é a realização de uma análise qualitativa sobre o que está a ser investigado, ao invés de recair sobre uma real medição de resultados. Afirma-se assim ser uma dissertação com uma filologia mais predominantemente interpretativa, tendenciosa ou fenomenológica.

O método de investigação baseia-se na leitura de bibliografia diversa dentro do domínio da investigação, estudos de caso, questionários, *workshops* e confronto/análise da realidade de algumas situações concretas. Foi efetuado um estudo alargado para identificação de legislação e regulamentos próprios, além disso foram estudadas diversas normas e boas práticas de forma a permitir a alusão exposta neste documento para a resolução do problema levantado pelo mesmo.

Através de estudos de caso disponibilizados sobre realidades de administração local a nível internacional é percetível a existência em algumas situações de um elevado grau de capacidade nos processos TIC, já com um sistema de governação estabelecido.

Neste trabalho foi efetuado, no decorrer da investigação, uma análise de capacidade dos processos TIC fundamentada no CobiT5, que permitiu atestar a necessidade urgente de capacitação de processos críticos e base, devendo para isso fazer-se uso de boas práticas já reconhecidas como eficazes.

1.5. Estrutura da dissertação

Esta dissertação consiste em cinco capítulos. O capítulo 1 Introdução pretende ser o local onde é apresentado o problema identificado, os objetivos a alcançar e a contextualização da solução de alto nível proposta, neste capítulo também é efetuada a alusão à forma de investigação seguida no desenvolvimento desta dissertação. O capítulo 2 resume o compêndio de literatura, trabalhos académicos, estudos de caso e normas que são utilizados na demonstração do problema e alinhamento à solução. O capítulo 3 apresenta o caso de estudo efetuado em parte fazendo a antevisão e preparação da solução proposta e apresentada no capítulo 4 que descreve as etapas levadas a cabo para validar a relevância da solução proposta para o problema levantado. No capítulo 5 é efetuado um resumo da dissertação, análise aos resultados percetíveis e relativos ao problema levantado assim como futuras investigações ou melhorias à investigação efetuada.

2. Trabalhos relacionados

Neste capítulo pretende-se apresentar trabalho relacionado com o tema da dissertação. Essencialmente é pretendido apresentar normas e *frameworks* existentes e que fazem parte de estruturas de governação e/ou gestão das TIC. Serão também apresentados casos conhecidos de aplicação de EGTIC na administração pública a nível internacional. Será também nesta capítulo dado a conhecer o plano geral para a redução de custos nas TIC por parte do governo Português.

2.1. Normas e *frameworks*

Nos dias de hoje existem normas e *frameworks* para quase tudo, sendo que as TIC e SI não são exceção. Durante a pesquisa de conhecimento sobre governação/gestão de tecnologias de informação, serviços e segurança foram identificados quatro *frameworks*/normas principais que depois na sua parcial aplicação levam a outras de interesse para esta dissertação. Assim, como principal e autoproclamada agregadora de todas, temos a *framework* CobiT 5 (*Control Objectives for Information and related Technology*) [10], de seguida, e das mais utilizadas em termos de sistemas de informação como *framework* de gestão de serviços TIC, temos a ITIL (*Information Technology Infrastructure Library*) [11]. Perfeitamente alinhada à ITIL existe a norma ISO/IEC 20000 para a gestão de serviços de tecnologias de informação [12], e no que diz especificamente só respeito à segurança, existe a família de normas ISO/IEC 27000 para a segurança da informação [13].

2.1.1. CobiT 5

O CobiT é uma framework criada pela ISACA[3] (*Information Systems Audit and Control Association*) para a gestão e governação de TI. Esta *framework,* é constituída por um conjunto de conhecimentos e ferramentas que auxiliam os responsáveis e governantes a efetuarem a ligação entre requisitos de controlo, questões técnicas e risco.

A ISACA foi instituída por um pequeno grupo de indivíduos que em 1969 sentiram a necessidade de centralizar conhecimento e guias na crescente área da auditoria a controlos de sistemas computacionais.

A versão 5 do CobiT foi lançado em Abril de 2012, e alterou completamente o conceito em relação à versão anterior que era a versão 4.1, pois integrou numa única ferramenta aquilo que a ISACA disponibilizava em várias, Val IT 2.0 (*Value IT Framework*), Risk IT, ITAF (*IT Assurance Framework)* e BMIS (*Business Model for Information Security*) assim como o próprio CobiT 4.1.

O CobiT foi assumindo ao longo dos tempos outras competências além daquelas competências iniciais de auditoria para as quais tinha sido idealizado, ver Figura 2.

[3] https://www.isaca.org/Pages/default.aspx

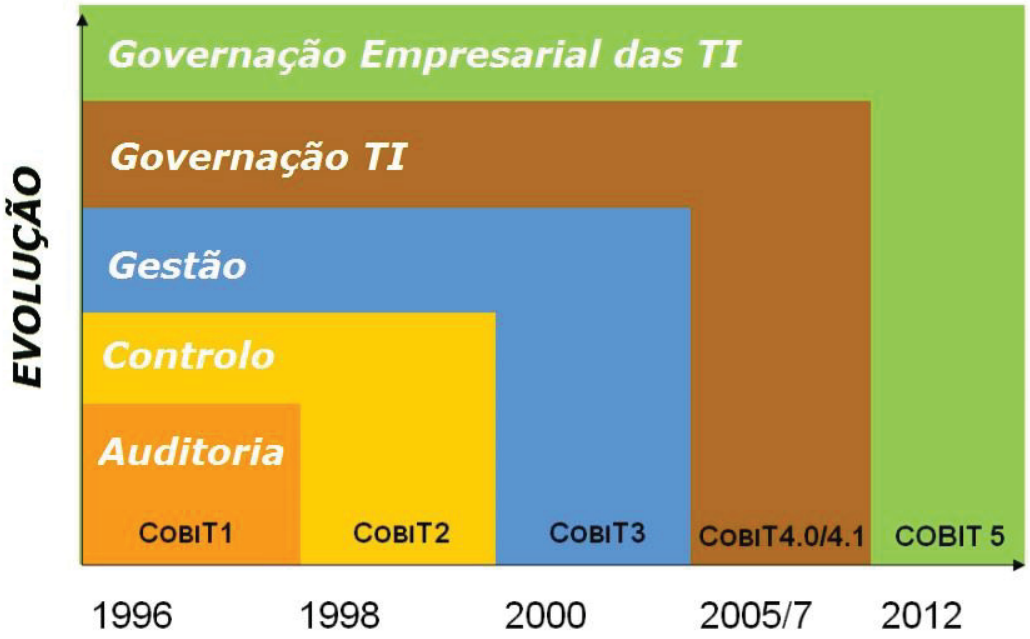


Figura 2 - Evolução do CobiT adaptado de [14]

O CobiT 5 atualmente é um completo conjunto de guias de facilitadores[4] e de implementação, convertendo-se numa *framework* adaptável ao ambiente a que se pretende implementar, sendo que é alinhável com os maiores *standards* e *frameworks* no mercado.

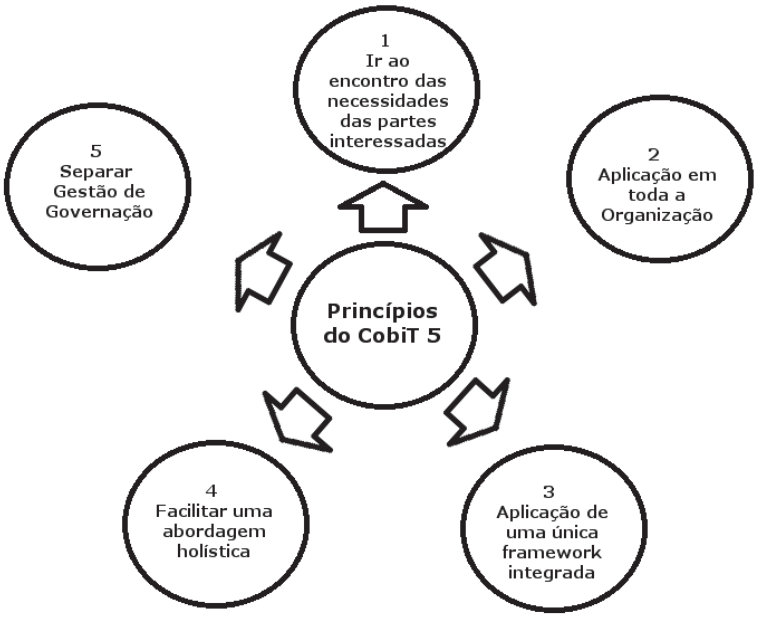


Figura 3 - Princípios do CobiT 5, adaptado de [8]

O CobiT 5 é baseado em cinco princípios, Figura 3, sendo eles:

[4] Mecanismos identificados pelo CobiT 5 que capacitam a mudança

1. **Ir ao encontro das necessidades das partes interessadas**: As organizações existem para criar valor para as suas partes interessadas, sendo que o objetivo da governação é a criação de valor baseada na realização de benefícios, otimização do risco e otimização dos recursos;
2. **Aplicação em toda a organização**: Integrar a governação das TIC na governação da própria organização, alinhar com a visão e cobrir todas as funções e processos dentro da organização;
3. **Aplicação de uma única *framework* integrada**: O CobiT 5 alinha com as últimas versões dos *standards* e *frameworks* mais relevantes utilizadas pelas organizações, (COSO, ISO/IEC 9000, ISO/IEC 31000, ISO/IEC 38500, ITIL, ISO/IEC27000, TOGAF, CMMI), sendo uma *framework* integradora de governação e gestão;
4. **Facilitar uma abordagem holística**: Existência de facilitadores (*Enablers*), descritos em 7 categorias, Figura 4, para apoio na implementação de uma governação e gestão global das TIC.

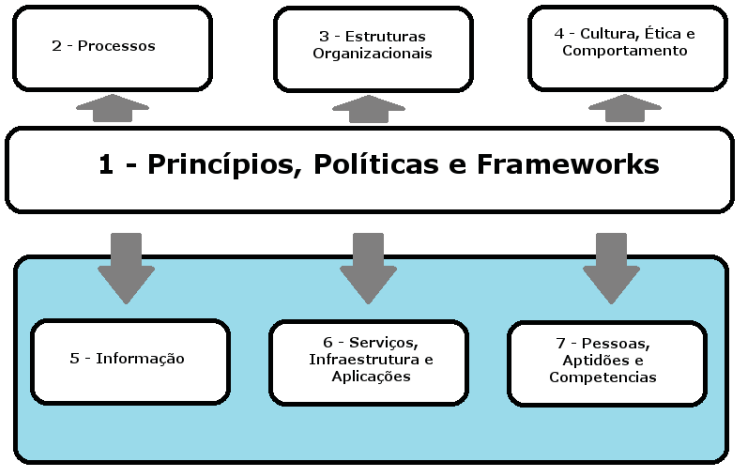


Figura 4 - Facilitadores do CobiT 5, adaptado de [8]

5. **Separar gestão de governação**: Distinção clara entre governação e gestão, em que cada uma delas implica diferentes tipos de atividades e requerem estruturas organizacionais diferentes que servem propósitos diferentes, ver Figura 5:
    a. Governação: Responsabilidade de direção sob um presidente. Deverá orientar, avaliar e monitorizar o domínio da gestão;
    b. Gestão: Responsabilidade de execução sob chefia. Deverá planear, construir, executar e monitorizar.

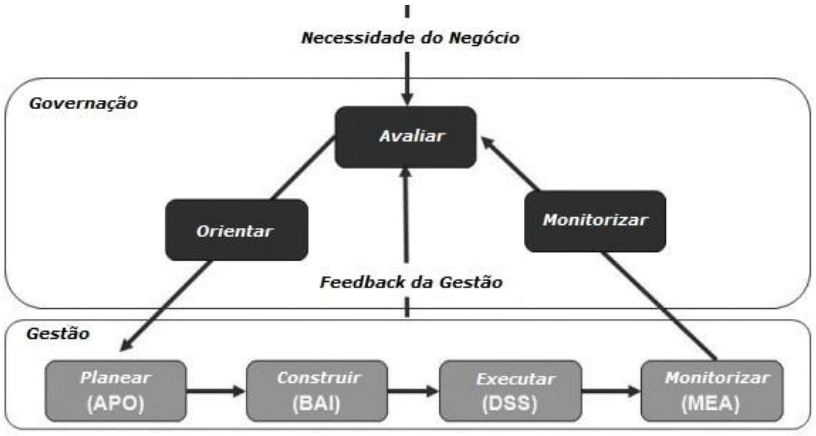


Figura 5 - Relacionamento entre domínios, adaptado de [8]

Dividido então em dois grandes domínios, o CobiT 5 identifica 37 processos de alto nível a ser capacitados. São os processos selecionados por encadeamento em cascada com cruzamento de objetivos TIC, da organização e partes interessadas (do inglês *stakeholders*), ver Figura 6, capacitados depois com o apoio dos facilitadores do CobiT 5, que irão melhorar de forma contínua até ao nível desejado todas as funções e processos TIC da organização.

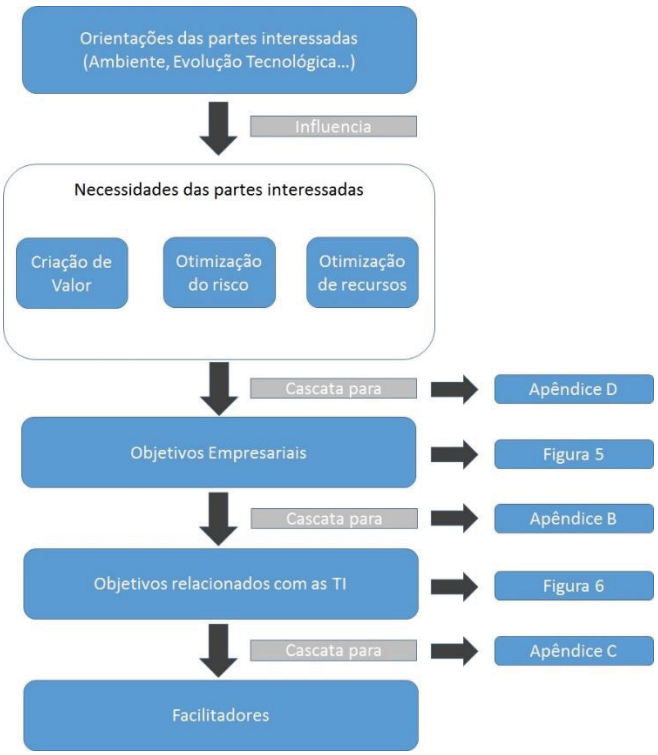


Figura 6 - Encadeamento de objetivos, adaptado de [8]

Note-se que na Figura 6, os apêndices e figuras referenciadas são as existentes na *framework* CobiT 5 [8] e não as existentes neste documento.

É com base neste processo de melhoria contínua que esta dissertação mostra a capacitação de processos TI, que mesmo não sendo concretamente para a segurança e garantia da informação, deverão reger-se pelas necessidades das partes interessadas, na garantia da informação que estes pretendem.

2.1.2. ITIL

A ITIL (*Information Technology Infrastructure Library*) tem vindo a evoluir ao longo da sua existência, desde a versão v1 até à atual v3, tendo havido na atual uma melhoria considerável nos processos chave, mas o mais importante é que também nesta última versão, a ITIL faz a descrição de funções de gestão de serviços, atividades e estrutura organizacional mostrando mais preocupações estratégicas assim como mais integração com o negócio.

A ITIL é uma livraria sobre a infraestrutura de tecnologias e sistemas de informação, conjunto de livros com indicações de boas práticas e linhas de orientação para uma boa implementação, gestão e controlo das mesmas.

No âmago do seu desenvolvimento em 1980 pela CCTA (*Central Computer and Telecommunications Agency*) agora convergido no OGC (*Office of Government Commerce*) do Reino Unido, esteve a necessidade de normalizar a forma de gerir todos os *data centers* do governo Britânico de forma a obter serviços comparáveis. Quando foi publicado, muitas outras organizações ao observar a sua eficiência e beneficio, começaram também a efetuar a sua implementação e uso. Hoje em dia a OGC afirma *"ITIL® as the world de facto standard for service management because of its widespread use—especially in European countries. It has now started to proliferate through Asia, Australia and South Africa as well!*". [15]

A ITIL é uma estrutura de cinco livros, Figura 7, para se aplicar no desenvolvimento e gestão de serviços ligados às TIC, mas como estrutura que é, também ela obedece a um esquema próprio.

Figura 7 - Estrutura do ITILv3, obtido de [16]

A ITIL é modelada em volta do ciclo de vida dos serviços que é comportado nos cinco livros da ITIL, e vai desde a estratégia para os serviços, desenho dos mesmos para o livro que define os processos de transição e depois os de operação e pretende conferir ao ciclo uma capacidade de melhoria contínua num outro livro, Figura 8. O livro Estratégia foca-se em verificar o valor (benefício/retorno) de uma alteração ao ambiente TIC (processos, serviços, tecnologia, pessoas) da organização, para isso deverá analisar os custos envolvidos e a necessidade de efetuar a mesma. No Desenho faz-se a definição dos itens de configuração que num conjunto poderão fazer parte da alteração (criação, mudança ou eliminação), levando em conta a disponibilidade e a continuidade do ambiente além de outras possíveis caraterísticas identificadas na estratégia. Na Transição é tratada a forma de aplicar as alterações desenhadas e coloca-las em produção de uma forma segura. As alterações após entrarem em produção deverão ser mantidas em funcionamento, sendo isso definido pelos processos e funções identificadas no livro de Serviços Operacionais. Os Serviços de Melhoria Contínua possuem o foco na mudança, apoiando a melhoria contínua de todos os serviços contidos nos outros livros da ITIL.

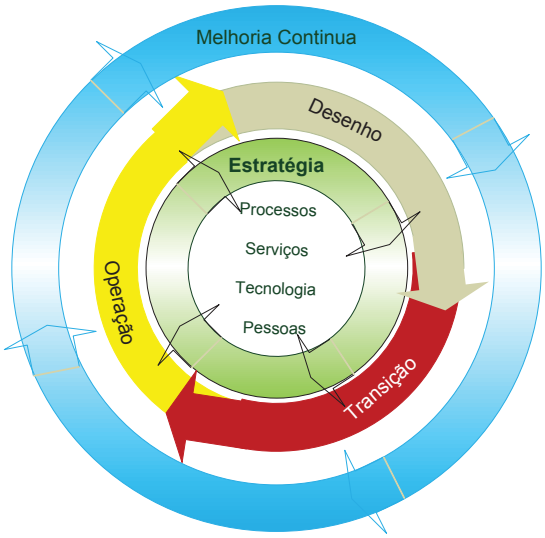


Figura 8 - Ciclo de vida ITIL v3, adaptado de [17]

A ITIL defende desta forma que um serviço possui um ciclo de vida próprio que tem início no desenvolvimento da sua estratégia, passa pela fase de desenho e depois pelas fases de transição e operação e tudo num processo de melhoria contínua atenta às mudanças no negócio.

A estratégia do serviço permite efetuar o alinhamento com o negócio, sendo então traduzida pelo desenho da arquitetura e normas. A fase de transição define apoiada nas duas fases anteriores quais os planos de transição e as bases que irão suportar a operacionalidade do serviço.

Cada livro apresentado no tópico anterior possui uma série de processos designados [18]:

- **Estratégia de Serviço**
  - Gestão da Estratégia – Definição do mercado e quais as ofertas a desenvolver. Quais os ativos estratégicos e preparação para a execução;
  - Gestão Financeira de TI – Realização da gestão e previsão orçamental, contabilidade das TI e formas de cobranças/pagamentos;
  - Gestão de Portefólio de Serviços – Composto por três componentes principais:
    - Serviços em desenvolvimento, novas ideias e novos desenhos;
    - Que serviços se encontram em produção;
    - Que serviços se encontram obsoletos.
  - É este processo que deverá gerir o ciclo de vida do serviço;

- Gestão da Procura – É este processo que faz com que os responsáveis pela gestão dos SI (Sistemas de Informação) e TI (Tecnologias de Informação) conheçam qual a procura ou necessidade da empresa/instituição em relação aos serviços de TI. O plano de necessidades e capacidade (balanceado) dentro da real necessidade do cliente.

- **Desenho de Serviço**
  - Gestão de Catalogo – Processo responsável pela manutenção do catálogo de serviços em operação, esta é a parte do portefólio disponível e visível ao cliente;
  - Gestão de Nível de Serviço – Manutenção, melhora e entrega da qualidade esperada. Faz uso dos SLA (*Service Level Agreement*), mede o desempenho e justifica os custos;
  - Gestão da Capacidade – Identificação das necessidades dentro da procura gerada pelo negócio. Balanceamento das necessidades reais;
  - Gestão da Disponibilidade – Responsável por avaliar e identificar os riscos e impactos de cada componente do serviço em caso de indisponibilidade;
  - Gestão da Continuidade do Serviço – Garantia da continuidade do negócio, gestão dos riscos e plano atualizado de continuidade;
  - Gestão da Segurança da Informação – Alinhar a segurança das tecnologias de informação com a segurança do negócio, garantindo que é efetivamente gerida em todos os serviços;
  - Gestão de Fornecedores – Responsável por gerir os fornecedores e prestadores de serviços, controlo da qualidade fornecida, análise dos contratos e garantia de ROI.
- **Transição de Serviço**
  - Planeamento e Suporte da Transição – Descrição do fluxo do processo de entrega de novos serviços ou alterações, assegura o cumprimento dos planos (projetos e transições);
  - Gestão de Alterações – Gerir todas as alterações de forma eficaz e eficiente de forma a causar o mínimo de impacto no negócio;
  - Gestão de Ativos e Configurações – Manutenção de um inventário atualizado de toda a infraestrutura TI, identificação e registo das configurações que compõem essa mesma infraestrutura;
  - Gestão de Versões e Instalação – Responsável pela autorização de instalação de todas as alterações aprovadas, novas implementações;

- Testes e Validação – Garantir a qualidade de serviços novos ou adaptados, focado na obtenção dos benefícios desejados dentro do SLA;
- Avaliação – Avaliar a alteração pretendida, testando os efeitos pretendidos e não pretendidos com a alteração;
- Gestão do Conhecimento – Permitir que a empresa/instituição melhore a qualidade das decisões tomadas, garantido que as informações sejam confiáveis, seguras e disponíveis durante todo o ciclo de vida do serviço.

- **Operação de Serviço**
  - Gestão de Eventos – Gestão de todos os eventos que ocorram na infraestrutura de TIC;
  - Cumprimento dos Pedidos – Uma via direta para que os clientes/utilizadores possam usar para pedidos diversos;
  - Gestão de Incidentes – Responsável pelo restabelecimento das operações de TI no menor tempo possível garantindo o SLA;
  - Gestão de Problemas – Minimização do impacto ao se encontrar a origem principal dos incidentes, corrigindo e prevenindo novas ocorrências;
  - Gestão de Acessos – Gerir todos os utilizadores e os seus acessos de forma segura e correta.
- **Melhoria Contínua de Serviço**
  - Medição e Controlo – Prever e reportar a performance do serviço em comparação com os níveis desejados;
  - Relatórios – Conversão de todos os dados disponíveis em vistas passíveis de análise e gestão;
  - Melhorias – Identificar e introduzir melhorias na gestão do serviço, focado na melhoria continua.

2.1.3. ISO/IEC 20000

A ISO/IEC 20000 foi a primeira norma ISO na área das TIC a ser editada pela ISO e apesar de não formalizar a inclusão das práticas ITIL, esta possui os seus processos de gestão completamente alinhados com os definidos dentro dos livros ITIL.

Esta norma define as melhores práticas de gestão de serviços TI e o seu desenvolvimento foi baseado na BS15000 com a intenção de ser completamente compatível com a ITIL, sendo a sua primeira edição em Dezembro de 2005. [19]

Na realidade aquilo que se percebe é que para as organizações que foram adotando as melhores práticas ITIL e que em determinada altura por necessidade imposta externamente ou para melhoria da sua imagem, decidem pela certificação dos serviços TIC, recorrem à certificação em ISO/IEC 20000 devido ao seu completo alinhamento.

A intenção da norma é a definição de um conjunto de melhores práticas de gestão de serviços TIC, garantir assim a correta e mais eficaz disponibilização dos serviços por parte dos responsáveis TIC, aumentando o reconhecimento pelos serviços de qualidade. O fundamento principal da dinâmica da norma reside na melhoria contínua baseada no ciclo de vida PDCA (*Plan-Do-Check-Act*).

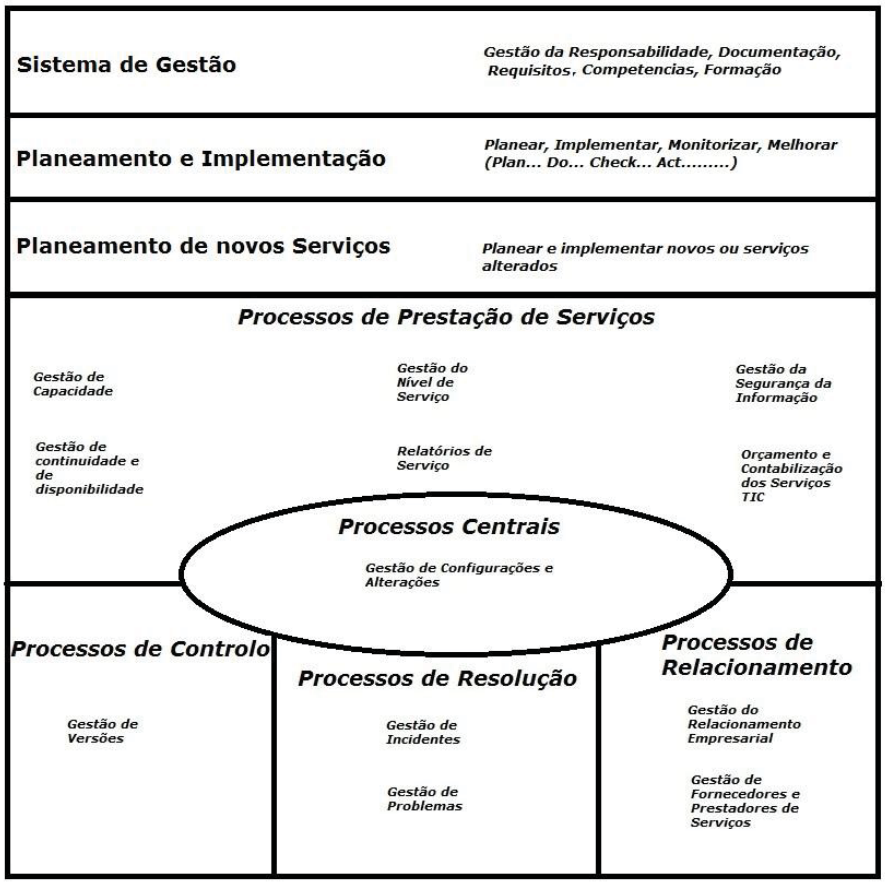


Figura 9 - ISO/IEC 20000, adaptado de [20]

A norma é composta de várias partes, entre as quais se destacam as principais:

- ISO/IEC 20000-1 que é a especificação formal e que define os requisitos para o sistema de gestão de serviços TIC, pode-se ver a sua abrangência na Figura 9 com todos os processos definidos e distribuídos em cinco grupos;

- ISO/IEC 20000-2 fornece a orientação sobre a aplicação do sistema de gestão de serviços TIC, inclui as melhores práticas para os processos de gestão definidos na ISO/IEC 20000-1;
- ISO/IEC TR 20000-3 que contém as orientações sobre a definição da abrangência de aplicabilidade da ISO/IEC 20000-3.

A ISO/IEC 20000-2 estabelece um conjunto de 8 capítulos, Figura 9, com práticas de referência em relação aos serviços de SI/TI:

- Sistema de Gestão: Estipula a necessidade de definição e implementação de um sistema de gestão, devendo incluir políticas, *frameworks* e outros processos e ferramentas que permitam efetivar os serviços de TIC nas organizações;
- Planeamento e Implementação: Identifica a necessidade de definição/realização de um processo de planeamento estruturado e sustentado para a gestão das TIC e SI com orientação à sua implementação e prestação;
- Planeamento de novos Serviços: Conseguir a garantia que novos serviços ou alterações a serviços existentes sejam alvo de gestão, fazer cumprir o acordado e estabelecido entre as partes envolvidas, nomeadamente ao nível dos custos e de qualidade;
- Processos de Prestação de Serviços: Assegurar que se encontram definidos, acordados, registados e geridos os diferentes níveis de serviço estabelecidos entre a organização e outras partes (fornecedores, clientes, parceiros);
- Processos de Relacionamento: Visam garantir que todos os envolvidos compreendem e alinham nas necessidades do negócio, compreendendo quer a capacidade quer os constrangimentos à disponibilização dos serviços acordados, além da aceitação das suas responsabilidades e obrigações;
- Processos de Resolução: Dotam as organizações de procedimentos e politicas que lhes possibilitam gerir processos de resposta a incidentes e prolemas verificados na disponibilização dos serviços TIC e de SI;
- Processos de Controlo: Têm o objetivo de assegurar a definição e controlo de componentes dos serviços e infraestruturas, mantendo igualmente a informação precisa de configurações;
- Processos Centrais: Garantir a prestação, distribuição e acompanhamento adequado ou mais alterações verificadas em ambientes de produção.

2.1.4. ISO/IEC 27000

O conjunto de normas ISO/IEC 27000 é na realidade o único realmente vocacionado e idealizado em prol da segurança em sistemas de informação. Na sua génese esteve um pedido do governo britânico mais concretamente pelo Departamento de Industria e Comércio. O CCSC (*Commercial Computer Security Centre*) foi encarregue de várias ações entre as quais a criação de critérios de avaliação de produtos de segurança TIC, além da criação do código de boas práticas para a segurança da informação. Um dos primeiros documentos foi o PD0003 dividido em 10 secções cada uma já contendo uma série de objetivos e controlos. [21]

A BSI (*British Standards Institution*) em 1995 e em continuidade do seu desenvolvimento publicou o primeiro *standard* verdadeiramente para a segurança da informação, desta feita com o nome de BS7799.

Em Dezembro de 2000 o BS7799 passa a norma ISO/IEC 17799. Entretanto uma outra norma que era a BS17799-2 que foi criada em 1998 pelo BSI passou em 2005 a ISO/IEC 27001, sendo que só em 2007 a ISO/IEC 17799 foi renomeada para ISO/IEC 27002 e passou a pertencer à família ISO/IEC 27000 que continua a crescer. [21]

Quando se fala na família de normas ISO/IEC 27000 normalmente existe a referência a uma certificação na norma ISO/IEC 27001 seguindo as boas práticas indicadas na ISO/IEC 27002, ou para a implementação de um SGSI (Sistema de Gestão da Segurança da Informação), sem esquecer que este *standard* é baseado num ciclo contínuo PDCA.

A ISO/IEC 27001 estabelece os requisitos para a implementação, gestão, documentação e melhoria contínua de um SGSI fazendo uso da gestão de risco (poderá ser pela ISO/IEC 27005). A equipa de implementação deve identificar, analisar e avaliar os riscos propondo a sua redução para níveis aceitáveis, sendo que a norma possui 130 controlos definidos que auxiliam nessa redução. [22]

A ISO/IEC 27002 disponibiliza um guia de implementação prático e informação mais concreta sobre cada um dos controlos identificados na ISO/IEC 27001, tal como quais os mais apropriados para implementação e quais os essenciais para conformidades legislativas. [22]

Na Figura 10 pode ver-se a estrutura de procedimentos e políticas que a ISO/IEC 27002 guia para implementação define.

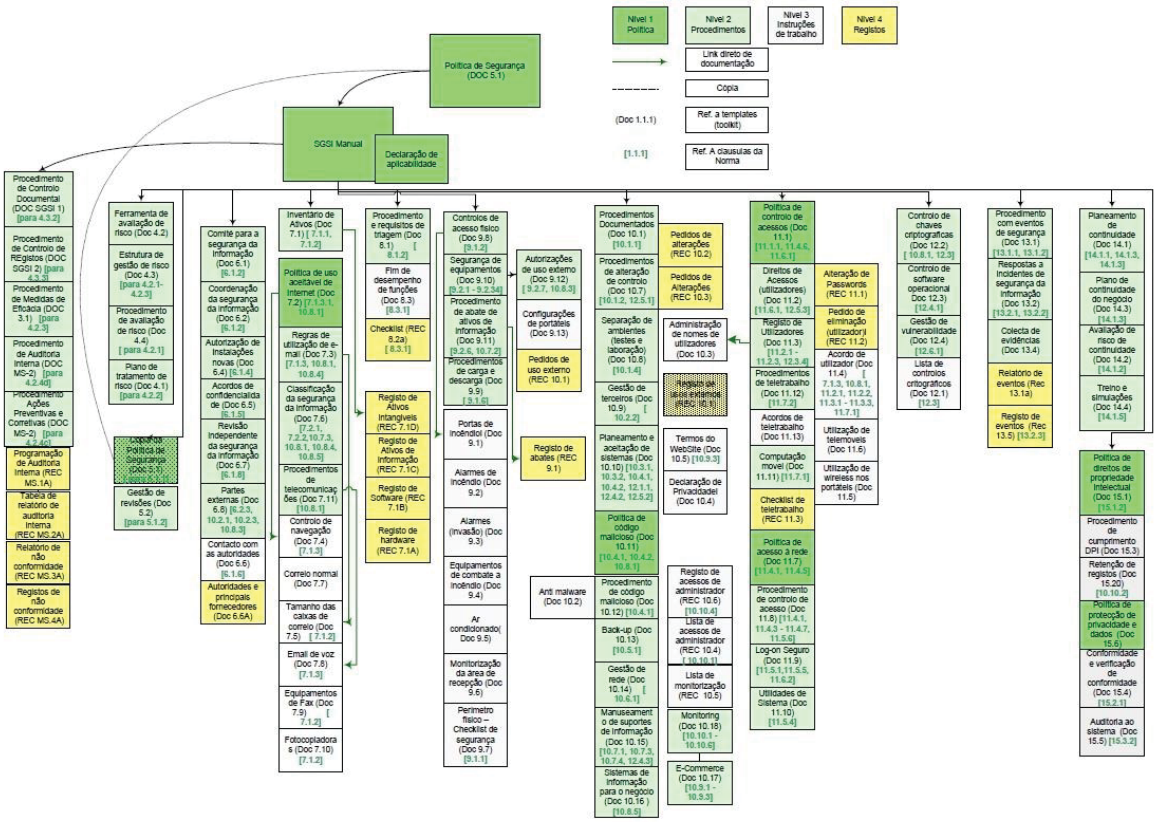


Figura 10 - Estrutura Procedimentos e Políticas ISO/IEC 27002

De realçar que qualquer organização que pretenda a certificação na ISO/IEC 27001, não necessita obrigatoriamente de seguir a implementação dos controlos indicados na ISO/IEC 27002, apesar de estes ao serem entregues mapeados como no anexo A da ISO/IEC 27001 facilitem a implementação. Por outro lado é possível adaptar os controlos às necessidades específicas de cada uma, até mesmo estendidos.

2.2. EGTIC na administração pública

Neste tópico abordar-se-á os sistemas de governação na administração pública a nível internacional, a sua aceitação e integração na forma de estar e ser, e descrever também uma eventual aproximação a este paradigma por parte do governo português.

2.2.1. Contexto internacional

A necessidade de implementação de sistemas de governação das TIC tem sido reconhecida e implementada a nível internacional de uma forma bastante ampla e a diferentes níveis e formas de integração.

Um caso de reconhecido valor e integrado a todo o nível da função pública e entidades privadas por organização central, é o da África do Sul com a emissão do relatório King III [23] e o esforço demostrado pelas organizações em o seguir.

"*With the increasing dependence on IT in modern enterprises and the significant risks associated with omnipresent IT systems in business, IT governance is becoming imperative to all organisations. King III is based on the "apply or explain" approach, that forces South African entities for the first time to apply the IT governance principles as contained in the report….*" [24]

"*In South Africa the Third King Report on Corporate Governance (King III) introduced 'The governance of IT' applicable to both private and public sector entities.*" [25]

O relatório King III foi lançado em Setembro de 2009 na África do Sul, este pretende ser reconhecido internacionalmente no que respeita a princípios da governação organizacional. A versão III é inovadora em relação à anterior por introduzir a governação das TI, a aplicabilidade a todos os tipos de organizações e a responsabilidade social imposta. [25] O relatório define no capítulo 5 sete princípios de governação que as organizações sul africanas deverão adotar.

Princípios	**Explicação**
5.1	O executivo deve ser responsável pela governação das TI
5.2	As TI devem ser alinhadas com a performance e os objetivos de sustentabilidade da organização
5.3	O executivo deve delegar na gestão a responsabilidade pela implementação de uma estrutura de governação das TI
5.4	O executivo deve monitorizar e avaliar os investimentos e despesas significativas em TI
5.5	As TI devem fazer parte formal da avaliação e gestão de risco da organização
5.6	O executivo deve garantir que os ativos de informação são geridos eficientemente
5.7	Uma comissão de risco e de auditoria deverá assessorar o executivo com as responsabilidades de TI

Tabela 1 - Princípios de Governação TI no King III, obtido de [25]

As administrações locais na África do Sul são assim obrigadas a melhorar a prestação de serviços, ser rentáveis e a estarem atualizadas com as tendências tecnológicas. Depois de terem identificados as TIC como um elemento fundamental na gestão empresarial e, portanto, com a introdução da governação de TI no relatório King III, foi enfatizado que as administrações locais devem priorizar as TIC como um ativo importante e estratégico devendo ser incluído na determinação da visão e objetivos a determinar, assim como na análise e gestão de riscos. [25]

Já no Brasil pode-se analisar o ato originário: Acórdão nº 1.603/2008-TCU (Tribunal de Contas do Plenário) - Plenário, que levou a um relatório de levantamento de auditoria em governação de TI (TC nº000.390/2010-0) na administração pública e acaba com as seguintes propostas à Sefti (Secretaria de Fiscalização de Tecnologias da Informação) [26]:

- Manter ações que estimulem a conscientização da alta administração das instituições da APF (Administração Pública Federal) acerca dos conceitos, objetivos, indicadores, ações e estruturas de governação de TI;
- Defina e mantenha processo permanente e sustentável de acompanhamento da governação de TI na APF de modo a subsidiar os processos de fiscalização do TCU em TI, bem como subsidiar os processos de planeamento e controle da própria APF;
- Remeta, para cada uma das instituições integrantes da lista disponível no Apêndice IV deste relatório, relatório contendo sua avaliação individualizada de governação de TI e a comparação com os resultados consolidados do respetivo segmento de atuação, como forma de subsidiar o planeamento dessas instituições.

Depois no acórdão nº 2.308/2010-Plenário são feitas as seguintes recomendações aos órgãos superiores:

- Orientar as instituições sob sua jurisdição sobre a necessidade de a respetiva alta administração estabelecer formalmente:
    - Objetivos institucionais de TI alinhados às estratégias de negócio;
    - Indicadores para cada objetivo;
    - Metas para cada indicador;
    - Mecanismos que a alta administração adotará para acompanhar o desempenho da TI da instituição;
- Promover, mediante orientação normativa, a obrigatoriedade de a alta administração de casa instituição sob sua jurisdição estabelecer os itens citados.

E faz ainda as seguintes determinações à Sefti:

- Monitorize a adoção das providências recomendadas;
- Continue a monitorar o cumprimento das providências recomendadas no acórdão nº 1.603/2008 – TCU-Plenário;

- Desenvolva ações de estímulo à consciencialização da alta administração das unidades da APF acerca de conceitos, objetivos, indicadores, ações e estruturas de governação de TI;
- Defina e mantenha processo de trabalho permanente e sustentável de acompanhamento da governação de TI na APF, com fins de:
    - Subsidiar processos de fiscalização do TCU em TI;
    - Subsidiar processos de planeamento e controlo das unidades jurisdicionadas;
- Realize levantamentos regulares com coleta de evidências;
- Dê publicidade ao levantamento:
    - Feedback aos participantes;
    - Divulgação das informações consolidadas;
    - Divulgação dos dados coletados sem identificação individual dos respondentes.

No último relatório efetuado pelo Tribunal de Contas (TC 007.887/2012-4) referente ao estado da governação das TI na APF sobressai-se a seguinte conclusão:

"274. O levantamento de governança de TI 2012 revelou, de forma geral, melhoria da situação em relação ao levantamento de 2010. Contudo, ainda há instituições na faixa inicial de governança de TI, o que está distante do aceitável, tendo como referência os modelos de boas práticas de governança de TI e a legislação e a jurisprudência vigentes.

275. Nos aspetos relacionados à liderança de uma boa governança de TI, verificou-se evolução significativa da quantidade de instituições que estabeleceram os mecanismos basilares da estrutura de governança de TI, além do aperfeiçoamento daquelas instituições que já possuíam alguma estrutura. Os números apurados são animadores, haja vista indicarem que a alta administração tem entendido seu papel e sua importância no contexto da governança de TI.

276. Também houve evolução nos aspetos relacionados ao desempenho institucional na gestão e uso de TI e ao desenvolvimento interno de gestores de TI. Contudo, causa preocupação que ainda existam instituições que não definiram objetivos, indicadores e metas de TI (item 9.1 do Acórdão 2.308/2010-TCU-Plenário), pois isso inviabiliza sua própria avaliação de desempenho.

…

285. Diante do cenário levantado, percebe-se que há espaço para melhorias, o que justifica a continuidade das ações do TCU no sentido de alavancar a governança de

TI na APF, e, sobretudo, dos levantamentos de governança de TI, que, além da ação indutora, permitem verificar a evolução da situação ao longo de um período e direcionar as ações posteriores. ” [27]

A preocupação do governo brasileiro com a melhoria de todos os processos relacionados com as TIC através da implementação de estruturas de governação TIC na APF é uma evidência. Conseguem assim melhorias orçamentais com custos controlados, além da uniformização de métricas que permitem melhores controlos e auditorias ao sistema. Por trás destes objetivos, podem-se também evidenciar as questões de segurança e obtenção de dados válidos.

Continuando a nível internacional, mas agora com foco na administração local, existem alguns exemplos interessantes que se podem enumerar.

A cidade de Houston é a mais populosa do estado do Texas e a quarta mais populosa dos Estados Unidos da América, possui uma área total de 1.625 Km^2 e uma população de 2.161 milhões de pessoas. A 20 de Dezembro de 2012 a ordem executiva n.º 1-44 com o assunto: "*Information Techonology (IT) Governance*" estabelece formalmente a sua estrutura de governação de TI. Na ordem executiva são definidas as comissões e responsabilidades, os princípios além do propósito e objetivos. Os processos que farão parte desta estrutura prendem-se com o alinhamento ao negócio, gestão de investimentos, gestão do risco, gestão da performance e a conformidade.

A cidade de Austin não possuindo as dimensões de Houston, é no entanto a capital do estado do Texas, com 704 Km^2 e 842.592 habitantes, também é um exemplo onde a governação das TIC é considerada uma mais-valia na garantia dos seus propósitos. Com esta estrutura de governação TIC pretendem estabelecer um processo de tomada de decisões transparente, informado e eficiente em relação aos serviços e necessidades, ao mesmo tempo que incentivam à participação dos parceiros e demais partes interessadas. [28] Na sua estratégia para as tecnologias de informação para o prazo 2012-2017 [29] no sumário executivo é logo referido que o pretendido é tornar disponível a informação certa, às pessoas certas, no momento exato por forma a permitir que estes possam tomar decisões corretamente informadas sobre as suas vidas, negócios, comunidades e governação.

Ainda no estado do Texas, podemos encontrar a cidade de *San Antonio*. Esta cidade possui uma área total de 1.205 Km^2 e 1.383 milhões de habitantes. No seu plano estratégico para as TI [30] onde a governação das TI define a forma como as decisões

em relação à priorização, seleção, orçamentação, planeamento, implementação e gestão das TI serão tomadas. Esta estrutura determina:

- Que decisões têm de ser tomadas para garantir a gestão e utilização eficiente das TI;
- Quem deve tomar essas decisões;
- Como é que essas decisões serão tomadas e monitorizadas.

No plano estratégico é descrito que com a implementação da EGTIC, o município garante benefícios através de um formato comum, conhecimento partilhado e controlos comuns para projetos e serviços.

O estado do Minnesota, também nos Estados Unidos da América com cerca de 5.303.925 habitantes e 206.232 Km^2 criou formalmente em Junho de 2012 uma estrutura de governação de TI [31]. Na introdução do documento que estabelece a estrutura de GTIC é logo definida a visão para a mesma "*IT governance exists to inform and align decision making for information technology planning, policy and operations in order to meet business objectives, ascertain that risks are managed appropriately and verify that resources are being used responsibly and strategically.*" [31] Com esta abordagem, alegam conseguir as operações diárias garantindo o nível de risco apropriado nas TI.

No Canadá, a sua capital *Ottawa* que possui uma área de 2.778 Km^2 e uma população de 883.391 habitantes na sua visão para as TIC expressa no seu *roadmap* tecnológico para 2013-2016 [32] não identifica diretamente a constituição de uma estrutura de governação, mas os princípios pelos quais se rege são inequivocamente os mesmos. Inclusive a própria existência do *roadmap* tecnológico já é uma evidência de uma estrutura governativa para as TIC, e forma de garantir a melhor e necessária informação às partes interessadas.

Em Inglaterra, no município de *Brighton and Hove* que possui uma população de 273.400 habitantes numa área de 8.754 Km^2, foi desenvolvida uma estratégia para as TIC do município que passa pela implementação da EGTIC [33] ao estabelecerem uma coleção de estruturas para as tomadas de decisão com a representação das outras áreas do negócio. Providenciam assim um ambiente para a gestão efetiva das TIC no qual os objetivos propostos para a organização poderão ser alcançados. Este processo fornece à gestão das TIC uma forma de tomada de decisão mais rápida ao remover a dependência da estrutura hierárquica. Ao incluir os munícipes num processo mais holístico de tomada de decisão que é ao mesmo tempo consistente e

transparente, os relacionamentos serão melhorados e as soluções melhor alinhadas com o negócio e as necessidades dos munícipes.

2.2.2. Contexto nacional

Em Portugal no ano de 2012 foi elaborado o PGERRTIC (Plano Global Estratégico de Racionalização e Redução de custos nas TIC, na Administração Pública) [34]. Este plano enumera cinco grupos de medidas importantes a aplicar aos recursos TIC na administração pública, sendo eles:

A. Melhoria dos Mecanismos de *Governance*;
B. Redução de Custos;
C. Utilização das TIC para Potenciar a Mudança e a Modernização Administrativa;
D. Implementação de Soluções TIC Comuns;
E. Estimulo ao Crescimento Económico.

No âmbito da garantia da informação e subsequente necessidade de segurança da informação este plano é baseado no grupo A que se subdivide nas seguintes medidas:

A. Melhoria dos Mecanismos de *Governance*
    - Definição e implementação da *Governance* das TIC na Administração Pública;
    - Racionalização, organização e gestão da função informática;
    - Arquitetura, normas e *guidelines* de tecnologias e sistemas de informação;
    - Definição e implementação de uma estratégia nacional de segurança da informação;
    - Definição e implementação de planos de ação setoriais de racionalização das TIC.

Destaca-se então aqui já a intensão e reconhecimento do governo português na importância do estabelecimento de estruturas de governação das TIC, sendo que no PGERRTIC também se pode ler que só o estabelecimento da governação das TIC na AP (Administração Pública) assegurará a sustentabilidade das medidas nele previstas, entre as quais a estratégia nacional de segurança da informação.

Em resposta de forma crítica ao PGERRTIC, a APDSI (Associação para a Promoção e Desenvolvimento da Sociedade da Informação) na 13ª tomada de posição do GAN (Grupo de Alto Nível) em 11 de Abril de 2012 na sala do senado na Reitoria da Universidade Nova de Lisboa, veio entre outros aspetos, reiterar a mesma ideia desta

dissertação na questão da priorização na implementação urgente de um modelo eficaz de governação das TIC na administração pública. [35]

Na sua tese [36] "*Improving the IT Strategic Plan for the Public Administration in Portugal*", Diogo Nunes, propõe melhorar o PGERRTIC ao proceder à sua implementação baseado em *frameworks* e boas práticas como é o caso do CobiT. Ele demonstra que a aplicação de uma linguagem comum e ferramentas do CobiT dentro do ciclo de vida definido pelo mesmo, melhoram o entendimento e facilitam a aplicação do PGERRTIC.

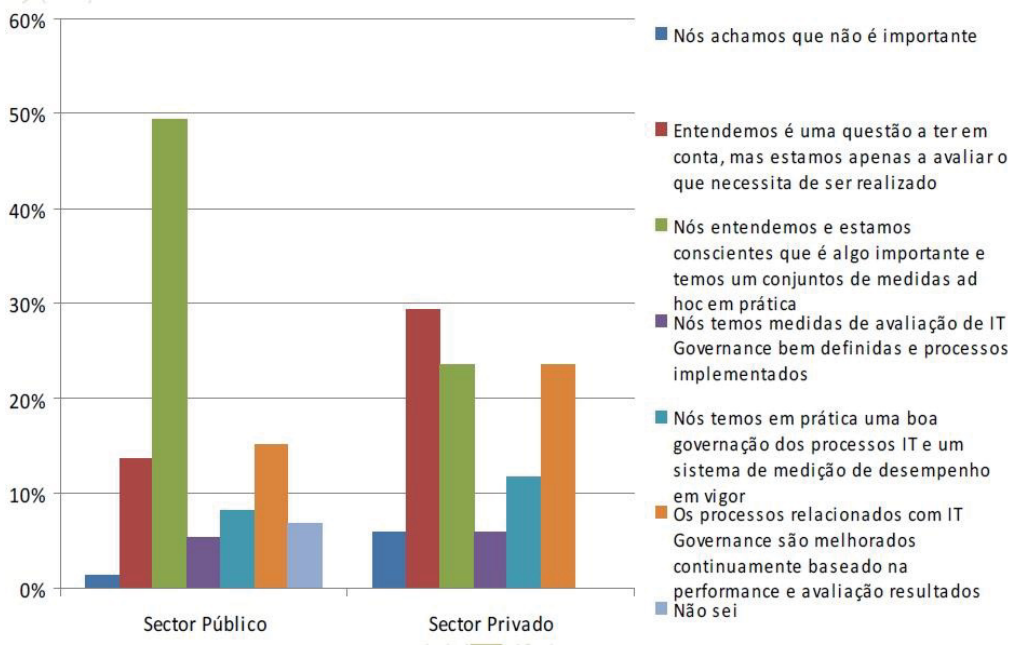


Figura 11 - Grau de Maturidade da Governação TIC em Portugal, obtido de [37]

Segundo o itSMF[5] (*The IT Service Management Forum*) sobre o grau de maturidade da governação das TIC em Portugal existe uma grande discrepância entre o setor público e o setor privado, ver Figura 11, no que respeita ao grau de maturidade do processo de governação TIC, sendo que se nota uma maior preocupação na gestão da continuidade no privado, sendo que no público existe a preocupação mas as medidas são ad hoc.

[5] http://www.itsmf.pt/ Fórum que reúne mais de 3000 organizações TIC no mundo

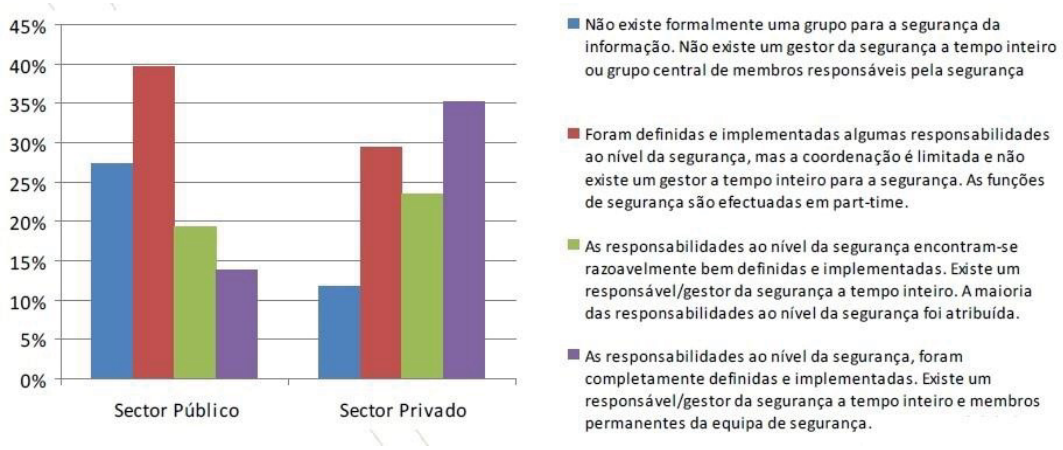


Figura 12 - Gestão da Segurança da Informação, obtido de [37]

Em relação à segurança, o itSMF, Figura 12, identifica uma maior preocupação do setor privado no estabelecimento formal das responsabilidades e gestão da segurança da informação, componente importante para a garantia de informação.

3. Proposta de implementação da EGTIC

Este capítulo apresenta, baseado no guia de implementação do CobiT 5 [4], a proposta para a implementação da EGTIC no município. Este guia propõe a realização de uma análise da capacidade do município antes de iniciar a implementação da EGTIC. De seguida é apresentado um programa de implementação de uma estrutura de governação[6], e ao mesmo tempo é efetuada a primeira iteração do ciclo de melhoria contínuo. Este ciclo irá dar início à capacitação dos processos do município, incluindo os processos relativos à segurança e garantia da informação.

[6] Devido ao apoio superior do executivo camarário e à necessidade de monitorização, a própria implementação da EGTIC deverá ser executada dentro de um programa pré-definido

3.1. Uso do guia de implementação

O guia de implementação do CobiT 5 [4] é um documento extenso que apoia, usando as ferramentas disponibilizadas pelo próprio CobiT para a implementação, a capacitação e melhoria contínua de todos os processos inerentes à governação e gestão das TIC numa organização. Este também orienta o programa de implementação para o seu arranque e a forma de concretizar cada uma das fases do ciclo de melhoria contínuo, incluindo a forma de utilizar outras ferramentas tais como o ITIL ou a ISO/IEC 27000.

3.1.1. Estrutura do guia

- *Chapter 1. Introduction:* Neste capítulo é efetuada uma introdução ao documento em si e à família de guias do CobiT 5 e da própria *framework*. É apresentado o âmbito do guia de implementação assim como os seus objetivos.
- *Chapter 2. Positioning GEIT:* Este capítulo apoia na compreensão e contextualização da posição da governação das TIC como sendo um elemento "empresarial" por si só. Este capítulo auxilia no levantamento do ambiente existente e do necessário para a implementação de uma EGTIC. São definidos os termos de governação das TIC, qual a sua importância e o que esta deve oferecer à organização. Aqui também é indicado como aproveitar o COBIT 5, integrar *frameworks*, normas e boas práticas.
- *Chapter 3. Taking the First Steps Towards GEIT:* Neste capítulo são indicados quais os primeiros passos a efetuar para iniciar o programa de implementação da EGTIC, tais como:
    - Criar o ambiente apropriado;
    - Aplicar uma abordagem de um ciclo de vida de melhoria contínua;
    - Identificar a necessidade de agir: Reconhecer pontos críticos e elementos despoletadores;
    - Reconhecer os papéis e requisitos das partes interessadas.
- *Chapter 4. Identifying Implementation Challenges and Success Factors:* Neste capítulo são indicadas as formas de gerir e criar o ambiente apropriado pela identificação pela experiência dos desafios e fatores críticos em cada fase do ciclo de melhoria contínua.
- *Chapter 5. Enabling Change:* Neste capítulo é fornecido apoio para facilitar a necessidade de mudança e como através desta é possível criar o ambiente facilitador para a implementação.
- *Chapter 6. Implementation Life Cycle Tasks, Roles and Responsibilities:* É neste capítulo que são estabelecidas as tarefas, papeis e responsabilidades

para cada fase da implementação e que são usados mais à frente nesta dissertação, secção 4.3.

- *Chapter 7. Using the COBIT 5 Components:* Neste capítulo são feitas considerações ao CobiT 5 e ferramentas que este utiliza.

Nas seções seguintes são apresentados os resultados da utilização de alguns destes capítulos, relevantes para o objetivo deste trabalho de investigação.

3.2. Análise da capacidade do município

Atualmente, no município, não existe uma estrutura bem definida para a governação das TIC, nem mesmo a utilização de melhores práticas (*frameworks*) tais como o ITIL, COBIT ou normas (*standards*) como o (ISO/IEC 27000, ISO/IEC 20000 ou ISO/IEC 38500:2008), são levadas em conta. Estão identificados alguns processos avulso que não têm o adequado nível de implementação levando a que no dia-a-dia não seja prático a sua utilização. Na prática, tem sido dada muito pouca atenção ao nível de capacidade dos processos nas TIC, sendo que com base na experiência ver Apêndice 1 - Análise de Capacidade, este é muito baixo.

Para atingir os objetivos identificados na secção 1.3 (Objetivos) do presente documento, para a implementação de uma EGTIC é necessário aumentar o nível de capacidade e de adequação dos processos e controlos das TIC.

O resultado deverá ser a identificação e articulação de uma parte significativa do risco, sendo possível geri-lo e efetuar relatórios sobre o seu estado. Com o aumento do nível de capacidade dos processos, o perfil de risco associado às TIC deverá diminuir, aumentando a qualidade e eficiência de forma proporcional dos processos relacionados com as TIC.

Em última análise, o valor do negócio (garantia de informação, transparência, atendimento e relação com o munícipe, eficácia, eficiência, igualdade e inclusão, etc) deverá aumentar como resultado de uma EGTIC eficaz.

Das boas práticas identificadas e reconhecidas internacionalmente, aquela que parece preocupar-se de forma mais transversal e holística com todo o processo governativo e de gestão das TIC e SI é o CobiT 5. No entanto, não deixa de ser uma solução proprietária e que nos pormenores remete para a leitura de outras mais especializadas (ITIL, ISO/IEC 27000, ISO/IEC 15504[7], etc). Esta situação e depois de comparar os aspetos específicos das várias boas práticas existentes, optou-se por usar o guia de implementação do CobiT 5 [4] auditar o sistema existente baseado na

[7] Também conhecida por SPICE, apoia na avaliação de capacidade dos processos

estrutura de processos identificados no CobiT 5 [8] e escolher os processos a capacitar seguindo a *framework,* Figura 6, e depois dentro dos processos escolhidos para capacitar, recorrer a apoio mais específico das diferentes normas e *frameworks* para os mesmos. Assim espera-se que seguindo as boas práticas e normas internacionalmente reconhecidas, e capacitando os processos identificados na aplicação dessas práticas e normas, bem como usando soluções também por estas apontadas, se garanta de uma forma mais segura os ativos de informação.

3.3. Implementação da EGTIC segundo o CobiT 5

Já fazendo uso do guia de implementação do CobiT 5 [4], nas subseções a seguir ir-se-á abordar pontos importantes a levar em conta na implementação, tais como o reconhecer o contexto, como usar as ferramentas necessárias, a necessidade de criar o ambiente apropriado e como funciona o ciclo de melhoria contínuo do CobiT 5, Figura 13.

3.3.1. Reconhecer o contexto

O guia de implementação do CobiT 5 [4] no seu capítulo 2 - *Positioning GEIT*, subsecção 3.1.1, alerta para que a implementação de uma EGTIC não decorra no vácuo, esta deverá acontecer dentro de diversas condições e circunstâncias associadas e determinadas por inúmeros fatores internos e externos tais como:

- Ética e cultura;
- Legislação, regulamentos e políticas;
- Normas internacionais;
- Práticas industriais;
- Ambiente competitivo;
- Organizativos:
    - Missão, visão e valores;
    - Políticas e práticas de governação;
    - Cultura e estilo de gestão;
    - Modelos para as funções e responsabilidades;
    - Planos de negócio e intenções estratégicas;
    - Modelo de operações e nível de maturidade.

Isto implica que para cada organização a implementação deverá ser diferente tal como o contexto de necessidades a ser conhecido e considerado no desenho de uma nova ou melhorada EGTIC.

Uma parte importante é o reconhecer que a GTIC não é uma disciplina isolada, mas na realidade faz parte integral da governação da organização. Enquanto que a

governação do município é conduzida primeiramente com o intuito de prestar um serviço de valor aos munícipes e restantes partes interessadas que exigem transparência e uma eficiente gestão do risco e do bem comum, as oportunidades, custos e riscos associados com as TIC exigem um dedicado, ainda que integrado, foco na GTIC. A EGTIC capacitará o executivo para obter todas as vantagens das TIC, maximizando benefícios e capitalizando oportunidades.

3.3.2. Usar o CobiT 5 e outras ferramentas

O apoio superior para a adoção e implementação de uma EGTIC é imperioso, e deverão ser seguidas as boas práticas reconhecidas. Deverá ser o executivo a mandatar a implementação da estrutura como parte integral do exercício governativo do município. A estrutura define a abordagem total à implantação, sendo então guiada pelos *standards* e boas práticas específicas para o desenho de políticas, processos, práticas e procedimentos. Ao se trabalhar com o CobiT 5 e alavancar as boas práticas, espera-se que os processos apropriados de governação, assim como outros facilitadores, possam ser desenvolvidos e otimizados. Assim, a EGTIC pode operar efetivamente como prática normal do município obtendo suporte cultural (passa a fazer parte da cultura da organização) demonstrado pelo executivo. O alinhamento ao CobiT 5, de acordo com, capítulo 2 - *Positioning GEIT* e capítulo 7 - *Using the COBIT 5 Components* do guia de implementação, subsecção 3.1.1, vai também apoiar na elaboração de auditorias mais rápidas e eficientes, visto este ser aceite como base de procedimentos para as auditorias TIC.

Toda a estrutura e os facilitadores que esta possa usar deverão estar em harmonia com as ferramentas e outros facilitadores existentes na organização, tais como as políticas, estratégias, planos de governação e abordagens de auditoria, sistema de gestão de risco, processos e estruturas de governação da organização.

3.3.3. Criar o ambiente apropriado

De acordo com o capítulo 3 - *Taking the First Steps Towards GEIT* e *5 Enabling Change* do guia, subsecção 3.1.1, a implementação de uma EGTIC é por si só uma iniciativa que deverá ser governada e adequadamente suportada e gerida. A maioria das iniciativas TIC acabam por falhar devido à inadequada orientação, gestão, suporte e supervisão.

A melhoria contínua e capacitação de processos nunca poderão fazer parte das práticas normais da organização sem uma estrutura de gestão que i) atribua papéis e responsabilidades, ii) se compromete na continuidade das operações e iii) monitorize a sua conformidade.

Para garantir a implementação da EGTIC como parte integral do sistema de governação do município é então necessário proporcionar o adequado ambiente à mesma. Isto inclui uma adequada direção e supervisão da iniciativa, incluindo os princípios guia, cujo objetivo é indicar o compromisso adequado e a direção e controlo das atividades para efetivamente haver um alinhamento com os objetivos do município.

As atividades iniciais normalmente incluem a avaliação do ambiente governativo, práticas correntes e o desenho de melhores estruturas. Em alguns casos poderá levar a alguma reorganização, assim como, a reorganização das próprias funções TIC na organização, incluindo a sua relação com as restantes UO, que neste caso passaria de uma relação de suporte para parceiro estratégico.

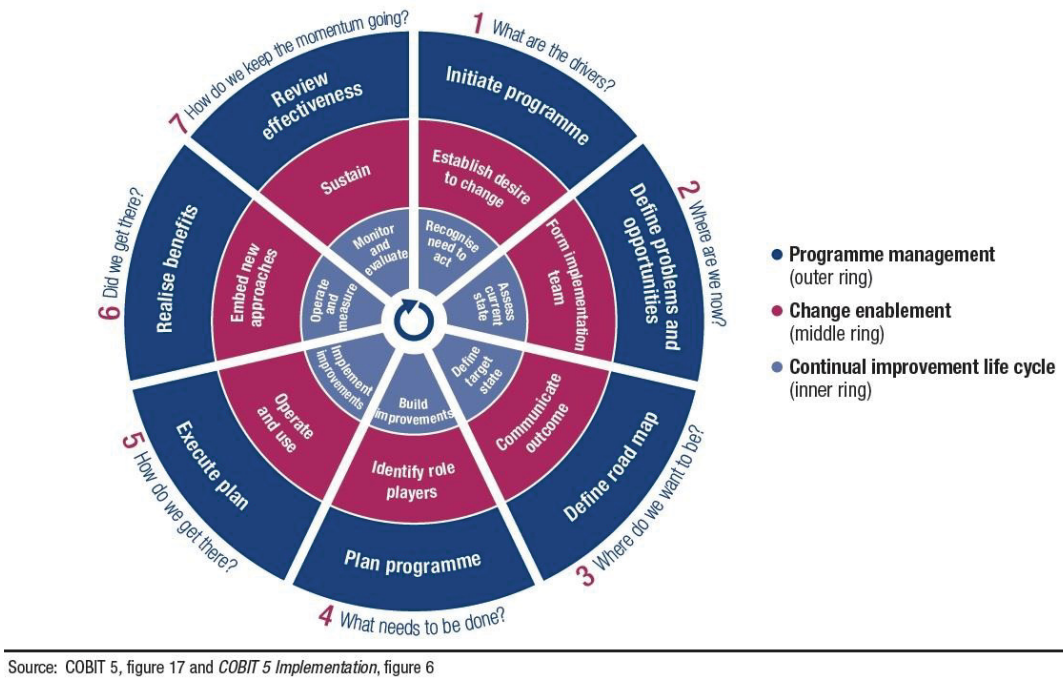
O executivo deverá proporcionar claramente apoio e alocar responsabilidades e papéis ao programa de implementação da EGTIC.

3.3.4. Ciclo de melhoria contínuo

O CobiT 5 proporciona uma abordagem de ciclo de melhoria contínuo como forma das organizações enfrentarem a complexidade e os desafios tipicamente encontrados durante a implementação de uma EGTIC. De acordo com o capítulo 3 - *Taking the First Steps Towards GEIT* do guia, subsecção 3.1.1, este ciclo encontra-se dividido em três componentes, (1) o componente central Melhoria Contínua (do inglês *Continual improvement life cicle*), (2) Facilitador da Mudança (do inglês *Change enablement*), preocupado com os aspetos culturais e comportamentais, ver Figura 4, e (3) a gestão do programa (do inglês *Programme Management*). As iniciativas são retratadas, Figura 13, para enfatizar o facto de não serem atividades pontuais, mas parte de um processo contínuo de implementação e melhoria que no decorrer do tempo se tornam parte dos processos do município, momento este em que o programa termina.

Cada um dos três componentes está dividido em sete fases, Figura 13, o programa de implementação e melhoria é tipicamente contínuo e interativo sendo que durante a última fase deverão aparecer novos objetivos e serão identificados novos requisitos para um novo ciclo.

Para dar início ao ciclo deverão ser usados resultados de auditorias, considerações na necessidade da iniciativa da GTIC e outros pontos a melhorar.



Source: COBIT 5, figure 17 and *COBIT 5 Implementation*, figure 6

Figura 13 - Ciclo de implementação EGTIC, obtido de [4]

Descrevem-se em seguida as fases conforme descritas no guia de implementação do CobiT 5 [4]:

- **Fase 1- O que nos Move?** Identificar as atuais necessidades de mudança e criar no executivo o desejo de mudança que deverá ser expresso numa justificação estratégica. Uma necessidade de mudança poderá ser um evento interno ou externo, condição ou problema chave que sirva como estímulo à mudança. Eventos, tendências (industriais, técnicas ou de mercado), falhas de eficácia, implementações de *software* ou mesmo os objetivos da organização podem agir como despoletadores da necessidade de mudança. O risco associado com a implementação do programa por si será descrito na justificação estratégica e gerido ao longo do seu ciclo de vida. Preparar, manter e monitorizar a justificação estratégica é fundamental e uma disciplina importante para justificar, suportar e então garantir o sucesso nos resultados de qualquer iniciativa, incluindo a melhoria da EGTIC. Esta garante um foco contínuo nos benefícios do programa e na sua realização;
- **Fase 2 – Onde nos Encontramos?** Alinhar os objetivos relacionados das TIC com as estratégias e risco da organização, priorizar os objetivos mais importantes da organização e os objetivos e processos relacionados com as TIC. Após o relacionamento entre os objetivos da organização e os das TIC, o CobiT 5 apoia na seleção dos processos que necessitam de ser capacitados para poder suportar o sucesso nos resultados. O sistema de gestão dos SI

necessita conhecer a sua capacidade atual e as deficiências que possam existir. Isto é alcançado através de uma análise à capacidade atual dos processos selecionados para capacitação;

- **Fase 3 – Onde queremos Chegar?** Definir as metas para as melhorias, seguida de uma análise às falhas por forma a identificar potenciais soluções. Algumas soluções serão de ganhos rápidos e outras mais desafiadoras e tarefas a longo tempo. A prioridade deverá ser dada a projetos que sejam de fácil alcance e com um maior benefício. As tarefas que possam ser de uma amplitude maior deverão ser divididas em tarefas mais curtas e facilmente geridas;
- **Fase 4** – **O que é Necessário Fazer?** Planear soluções exequíveis e práticas, definindo projetos apoiados em justificações estratégicas e desenvolvendo um plano de mudança. Uma justificação estratégica bem desenvolvida irá ajudar a garantir que os benefícios do projeto são identificados e monitorizados de forma contínua;
- **Fase 5 – Como Chegar lá?** Providenciar as práticas diárias de implementação, medidas a estabelecer para mensuração assim como sistemas de monitorização por forma a garantir o alinhamento com a organização. O sucesso requer o compromisso, consciencialização, compreensão e comunicação da gestão de topo assim como pelos proprietários dos processos de TIC;
- **Fase 6 – Chegámos lá?** Foca na transição sustentável do sistema de governação melhorado e das práticas de gestão na operacionalidade normal da organização. Monitorizar os resultados das melhorias utilizando métricas de performance e os benefícios expectáveis;
- **Fase 7 – Como manter o *Momentum Going*?** Rever a totalidade do sucesso da iniciativa, identificar novos requisitos de governação e gestão, reforçar a necessidade de melhoria contínua. Priorizar novas oportunidades de melhoria da EGTIC.

3.4. Implementação do programa

De acordo com o que está definido no *Appendix D* do guia de implementação [4] na etapa 2 a ver na secção 4.3 é necessário definir o programa de implementação de uma estrutura de governação, o que é feito nesta secção.

3.4.1. Âmbito do programa

O âmbito deste programa é definido pelas ações para o desenvolvimento de melhores práticas com vista ao aumento de capacidade dos processos existentes na gestão das

TIC do município e criação de processos de governação das TIC não existentes atualmente, dentro das competências da nova DMSI (Divisão de Modernização e Sistemas de Informação) [38] por forma a garantir que a informação é disponibilizada, tratada e armazenada de forma segura e em alinhamento com os objetivos do município.

A DMSI possui diversas competências divididas pelas seguintes áreas principais:

- Gestão de Projetos e Desenvolvimento Tecnológico;
- Administração de Sistemas e Infraestruturas;
- Inovação, Modernização e Gestão da Qualidade.

Sendo que umas competências são diretamente relacionadas com o suporte aos serviços existentes, outras estão intrinsecamente conectadas à estratégia do município pelo que os processos a capacitar deverão ser holisticamente transversais a toda a estrutura orgânica, Figura 14.

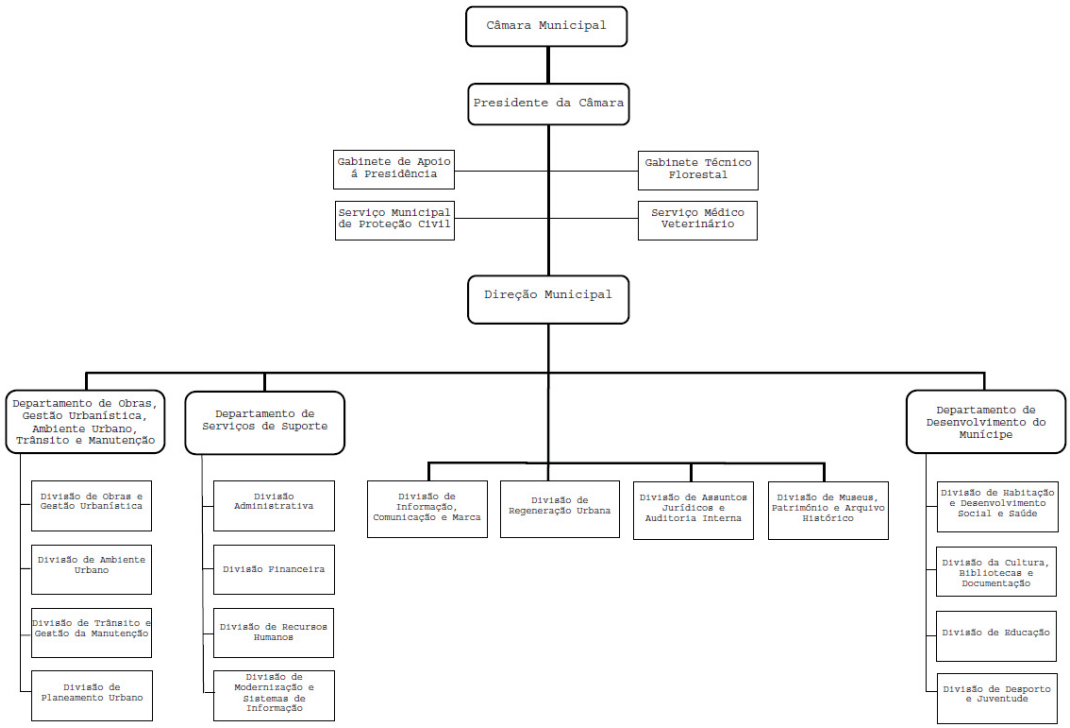


Figura 14 - Estrutura Orgânica da CMP, obtido de [38]

O município encontra-se situado no sul de Portugal possuindo uma área total de 182.1 Km^2 e uma população de 55.237 habitantes.

O município possui um complexo sistema de informação, ver Figura 15, que evoluiu ao longo dos anos e que é apoiado por um sistema tecnológico a necessitar de ser reestruturado, melhorado e modernizado. Além disso em termos de utilizadores o

município possui cerca de 1000 utilizadores dos diversos sistemas, espalhados por 43 localizações fisicamente distantes. Os servidores principais encontram-se no *data center* principal, havendo depois outros dois locais onde se encontram alojados serviços de informação. O parque informático encontra-se num estado não atualizável em termos de *hardware* desde há 4 anos, havendo equipamentos com 10 anos de funcionamento.

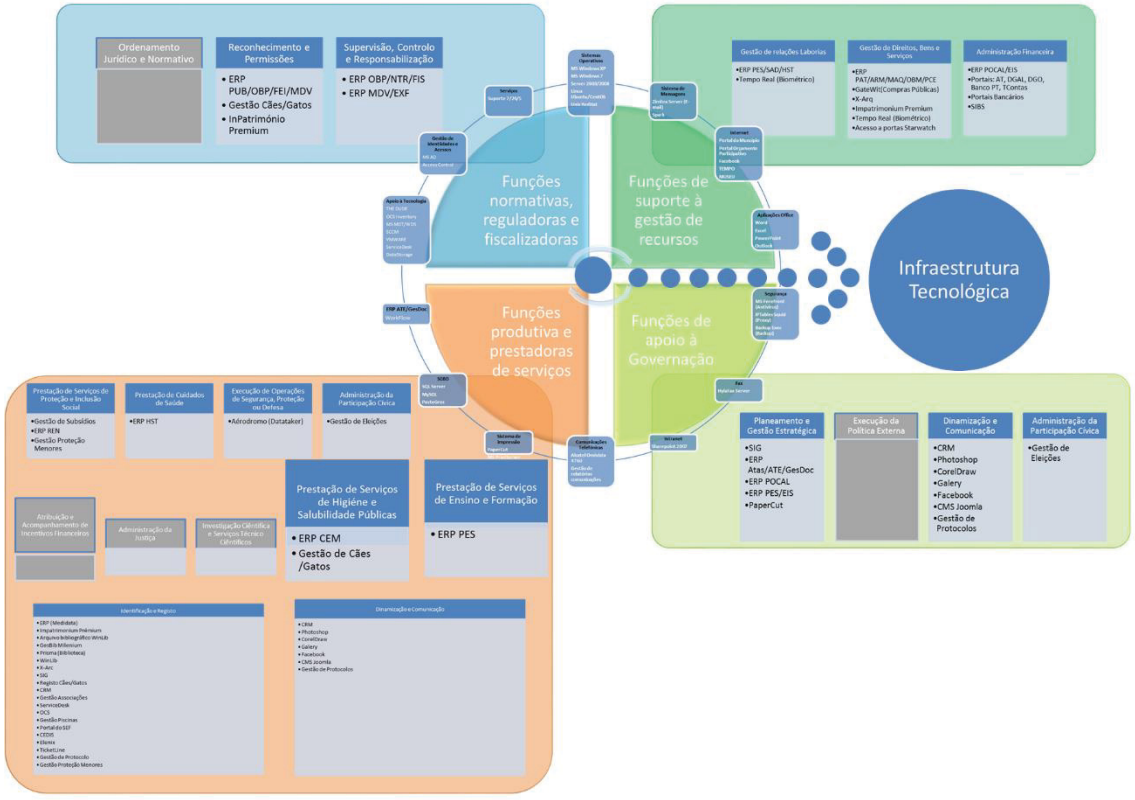


Figura 15 - Estrutura do atual Sistema de Informação

3.4.2. Metodologia e alinhamento do programa

Para alcançar os seus objetivos organizar-se-ão *workshops* interativos com todos os principais intervenientes para o sucesso do programa.

A abordagem deve garantir que os resultados do programa se encontram alinhados com os resultados esperados e prioridades do município.

Uma vez cobertos os objetivos do município, deve-se deslocar o foco para as operações das TIC, atualmente sob o controlo do CIO (*chief information officer*) do município, onde o risco e objetivos do negócio relacionados com as TIC serão analisados com mais detalhe.

Os objetivos do município, os objetivos das TIC, assim como as questões chave que dizem respeito ao cumprimento das necessidades das partes interessadas são então

combinados conforme indicado pelo encadeamento de objetivos definido pelo CobiT 5, ver Figura 6, que irá fornecer um conjunto de áreas a focar nos processos (CobiT) a ser tomados em consideração. Desta forma, será possível, ao município priorizar o esforço de correção para atender as áreas de risco nas TIC.

3.4.3. Resultados do programa

Como já mencionado, o objetivo global do programa de implementação da EGTIC é o de incorporar as boas práticas de governação das TIC, em contínuo, nas operações do município.

Serão produzidos resultados específicos por parte do programa que irão permitir ao município avaliar o cumprimento dos objetivos pretendidos pela EGTIC, incluindo os seguintes:

- Facilitar a partilha entre os colaboradores internos do conhecimento interno com recurso à plataforma de intranet, bem como o alavancar das relações existentes com fornecedores em benefício do município;
- Deverão ser criados relatórios detalhados sobre cada iteração de melhoria, devendo estes incluir:
    - Os objetivos atuais do município priorizados e os consequentes objetivos das TIC;
    - O risco identificado, associado às TIC, num formato *standard*, e as áreas acordadas para receber atenção baseada nos processos e melhores práticas definidos entre outros facilitadores recomendados;
    - O acima exposto, derivado das ferramentas de avaliação do programa de implementação da EGTIC.
- Relatórios gerais do progresso da implementação do programa;
- Relatórios consolidados que cubram:
    - Relatórios sobre os projetos acordados para implementação, baseados nas métricas de monitorização definidas;
    - Vista consolidada do risco TIC em todo o município;
    - Requisitos específicos da comissão de risco.
- Relatório financeiro das TIC;
- Implementar um mecanismo de monitorização de benefício e de relatórios sobre o valor dos objetivos e métricas definidas para o município.

Face a estes resultados e por forma a garantir que a informação existente é realmente necessária, que se encontra de acordo com o pretendido e disponível para quem dela necessita com a aplicação dos necessários e justos controlos de segurança, devem ser considerados alguns objetivos do programa como: i) melhor

prestação de informação através de relatórios e métricas de controlo; ii) melhoria dos métodos colaborativos de trabalho; iii) centralização e uniformização de projetos para priorização; iv) melhor enquadramento na arquitetura existente ou a desenvolver, e v) acima de tudo, a tomada de decisões ser baseada num definido ambiente governativo.

3.4.4. Riscos do programa de implementação

Existem potenciais tipos de risco para o sucesso inicial e em contínuo da implementação da EGTIC no município. Estes irão ser mitigados concentrando esforços na capacidade de mudança, e na sua constante monitorização e tratamento através de revisões ao programa e do registo de eventos de risco. Estes tipos de risco são:

- Compromisso do executivo e suporte ao programa;
- Demonstração do real valor criado assim como dos benefícios para o município resultantes da adoção do programa. Esta adoção deverá ser feita pela perceção do valor que poderá criar e não como resultado de alguma política imposta;
- Participação ativa do grupo das TIC na implementação do programa;
- Identificação das partes chave interessadas para participação no programa;
- A visão de negócio dentro da gestão da TIC;
- Integração com sucesso com outras iniciativas de governação ou de conformidade existentes no município;
- Existência de comissões com estruturas apropriadas para supervisionar o programa. Por exemplo, o progresso global do programa poderá fazer parte da agenda das reuniões da comissão executiva das TIC.

A análise e tratamento destes riscos por forma a maximizar a sua mitigação ou eliminação deverá ser feita na etapa 1 da implementação do programa que é analisada na secção 4.2 deste documento, e alavancados na fase 1 descrita na secção 4.3.

3.4.5. Análise custo/benefício do programa

O programa deverá identificar os benefícios esperados e monitorizar se está a ser criado valor real a partir dos investimentos realizados. Uma EGTIC racional deverá resultar em benefícios que serão definidos como metas específicas para o município, monitorizados e mensurados durante a implementação por forma a garantir o seguinte:

- Maximizar a concretização de oportunidades através das TIC, enquanto se mitiga o risco associado às mesmas para níveis aceitáveis, garantindo assim que o risco é responsavelmente ponderado em todas as iniciativas;
- Suportar os objetivos definidos pelo município através de investimentos chave e otimização do retorno dos mesmos, alinhando diretamente as iniciativas de TIC com as do município;
- Cumprimento legislativo, regulamentar e contratual, criação de políticas e cumprimento dos procedimentos internos dentro dos s*tandards* internacionais;
- Uma abordagem coerente para a medição e monitorização do progresso, eficiência e eficácia;
- Melhoria da qualidade dos serviços prestados;
- Custo reduzido das operações das TIC ou aumento da sua produtividade com a realização de um trabalho mais consistente em menos tempo e com menos recursos.

Os custos para cada iniciativa de projeto serão estimados na etapa 2 da implementação do programa, discutido na secção 4.3, e considerados caso a caso consoante o definido no documento de justificação estratégica. Assim será possível maximizar a eficiência e normalização na autarquia.

4.Solução

Neste capítulo serão descritas as atividades levadas a cabo no caso de estudo efetuado no município. Esta solução é baseada no *Appendix D. Example Business Case* do guia de implementação do CobiT 5 [4], assim como, as matrizes fornecidas pelo mesmo guia e pelo próprio *framework* [8]. Estas orientações são divididas em duas etapas, numa primeira etapa do programa pretende-se preparar o terreno e identificar necessidades, e na etapa 2 dar-se início ao ciclo de 7 fases de implementação do ciclo de melhoria contínuo do CobiT 5. No entanto é importante identificar os participantes que deverão estar envolvidos no programa, e que deverão ser partes interessadas chave no mesmo.

4.1. Identificação dos participantes

Foram identificados os seguintes participantes e ao mesmo tempo partes interessadas nos resultados da implementação do programa EGTIC:

- Executivo (Presidente ou representante);
- Direção e Chefias;
- Gestão das TIC (CIO e demais responsáveis);
- Serviços de Auditoria Interna;
- Comissão de Risco, Conformidade e Legalidade (incluir a Divisão Jurídica).

Será esta a composição proposta para a comissão de governação das tecnologias de informação e comunicação. A esta ir-se-á juntar a equipa responsável pela implementação do programa, durante o ciclo de implementação da estrutura, extinguindo-se após a conclusão com sucesso da mesma.

O programa necessita que as partes interessadas acima identificadas providenciem o seguinte:

- Orientação quanto à direção geral do programa de implementação da EGTIC. Inclui decisões sobre tópicos importantes relacionados com a governação bem como a definição de prioridades e a aprovação de objetivos de valor;
- Aceitação dos resultados e monitorização dos benefícios esperados do programa.

4.2. Etapa 1 – Pré-Planeamento – Ambiente apropriado

A etapa 1, e descrita no guia de implementação do CobiT 5 [4] como a de pré-planeamento do programa é a etapa de desenvolvimento do ambiente necessário para prosseguir com o programa. Durante esta etapa foram executados os seguintes passos:

Passo	Estado atual	Notas
Finalizar a estrutura da comissão de orientação do programa	Implementado	Está criada a equipa da comissão, sendo ela composta por 2 elementos da DMSI: Pedro Santos, Humberto Chula
Formação sobre as *frameworks* de governação à comissão de orientação do programa (poderá envolver consultoria externa)	Implementado	A formação nas *frameworks* é feita com recurso a informação recolhida pela equipa e de modo autodidata. Tem sido feita de forma contínua recorrendo a

		manuais e vídeos disponibilizados na web. Tendo levado a formação inicial cerca de um mês por forma a preparar a apresentação do primeiro workshop a toda a estrutura responsável pelas TIC no município
Workshop com a equipa de orientação para definir a abordagem para a autarquia	Implementado	A melhoria contínua da estrutura de governação das TIC no município será conseguida utilizando um ciclo de vida de implementação iterativo, constituído por sete fases: 1. O que nos move? 2. Onde estamos? 3. Onde queremos chegar? 4. O que feito é necessário fazer? 5. Como vamos lá chegar? 6. Já chegamos lá? 7. Como vamos manter o impulso? As iniciativas de mudança resultantes das fases serão baseadas nas boas práticas conhecidas, recorrendo a *frameworks* e *standards* de reconhecido mérito como são os seguintes: CobiT5, ITIL, ISO/IEC 20000, ISO/IEC38500, ISO/IEC/27000, ISO/IEC15504 entre outros
Criação de uma comunidade *on-line* na autarquia para funcionar como repositório para partilha de conhecimento	Parcialmente implementado	Nesta fase fica disponível um fórum no gestor de projetos, associado à implementação da EGTIC, e dirigido à DMSI. Foi implementado o Redmine[8] onde se encontram definidas todas as tarefas do programa, fórum, documentação e wiki
Identificação de todas as partes interessadas e das suas necessidades	Parcialmente Implementado	As partes interessadas foram identificadas, mas devido à reestruturação em curso não é possível aferir de forma completa e formal todas as suas necessidades
Clarificação e reajustamento, se necessário, das estruturas das atuais comissões, papéis e responsabilidades, regras de decisão e formas de prestação de contas (relatórios)	Parcialmente implementado	A comissão de orientação na implementação está criada, será durante a próxima fase que se pretende definir mais concretamente os papéis, regras de decisão e relatórios para KPI (*Key Performance Indicator*)

[8] http://www.redmine.org/ Gestor de Projetos

Desenvolvimento e manutenção do documento de justificação estratégica do programa para a implementação da EGTIC como base para o sucesso da iniciativa	Implementado	Documento Dinâmico que é "melhorado" de fase para fase em relação à evolução do ciclo contínuo de melhoria
Plano de comunicação para os princípios orientadores, políticas e benefícios esperados ao longo do programa	Parcialmente implementado	Apresentações aos interessados, reuniões e *workshops* com os intervenientes, gestor de projetos e fóruns abertos. Foram efetuadas apresentações iniciais sobre o pretendido e necessário às partes interessadas internas (exceto colaboradores). A elaboração de cada apresentação levou em média cerca de uma semana a ser concebida, pois dependia do público alvo
Desenvolvimento das ferramentas de avaliação e elaboração de relatórios para utilizar durante e após a implementação do programa	Parcialmente implementado	Só na fase (3) é que serão definidas as métricas e formas de medição para os resultados do programa.
Testar a abordagem numa situação menos complexa e realizar ajustes à mesma e às ferramentas utilizadas	Em curso	A escolha dos processos de prestação de serviço e suporte é também com o intuito de testar a abordagem e ganhar conhecimento dos *standards*
Efetuar um teste piloto numa situação complexa, já com a abordagem refinada. Servirá para perceber e quantificar as dificuldades na execução do programa em condições mais desafiantes, ainda em fase de avaliação	Não implementado	Fora dos objetivos desta dissertação pois exige um ciclo completo da etapa 2
Apresentação da versão final do programa, incluindo um plano de implementação, ao executivo da autarquia para a devida aprovação	Não implementado	Fora dos objetivos desta dissertação pois exige um ciclo completo da etapa 2

Tabela 2 - Passos da Etapa 1 da solução

4.3. Etapa 2 – Implementação do programa

Este programa foi concebido para iniciar um processo de melhoria contínua tipo PDCA (*Plan, Do, Check, Act*), com base no ciclo de vida iterativo seguindo as fases identificadas pelo CobiT 5 [8] e já definidas na seção 3.3.4. Seguindo o processo cada fase é dividida em três conjuntos de tarefas referentes a cada um dos três componentes: melhoria contínua, facilitador de mudança e gestão do programa, que terão determinadas entradas e saídas conforme o guia de implementação [4].

4.3.1. O que nos move?

Para iniciar esta primeira fase e após se terem identificado todas as partes interessadas, assim como elaborado algumas diligências para a criação do ambiente necessário no apoio ao programa, seções 4.1 e 4.2, passou-se ao levantamento dos dados/informações indicadas pelo CobiT 5 como necessárias nesta fase para se conseguir alcançar os resultados pretendidos para passar à fase seguinte.

Tipo de Tarefa	**Tarefas**
Melhoria Contínua	Reconhecer a necessidade de agir: 1. Identificar o atual contexto de governação, pontos críticos, eventos e sintomas despoletando a necessidade de agir; 2. Identificar as orientações de negócio e de governação assim como os requisitos de conformidade para apoiar na identificação das necessidades das partes interessadas; 3. Identificar as prioridades e as estratégias dependentes das TIC, incluindo qualquer projeto atual; 4. Alinhamento com as políticas, estratégias, princípios e iniciativas Organizacionais; 5. Sensibilizar o executivo da importância das TIC para a organização e o valor da GTIC; 6. Definir as políticas, objetivos, princípios e objetivos de alto nível para a GTIC; 7. Garantir que o executivo e diretores percebem e aprovam a abordagem de alto nível, aceitando o risco de não tomar nenhuma ação em questões significantes.
Facilitador da Mudança	Estabelecer o desejo de mudança: 1. Caso existam, garantir a integração com iniciativas de mudança em curso; 2. Analisar o ambiente geral da organização no qual a mudança necessita ser facilitada, incluindo a estrutura organizacional, estilo de gestão, cultura, formas de trabalhar, relações formais e informais e atitudes; 3. Determinar outras iniciativas em curso ou planeadas, por forma a identificar dependências ou impactos; 4. Perceber o impacto global da mudança; 5. Identificar as partes interessadas envolvidas na iniciativa das diferentes áreas do município; 6. Determinar o nível de suporte e envolvimento necessário de cada parte interessada, a sua influência e impacto na iniciativa de mudança; 7. Determinar a prontidão e capacidade para implementação das mudanças para cada parte interessada; 8. Estabelecer o ponto de partida, utilizando os pontos críticos e eventos iniciadores (*trigger events*) e comunicados pela comissão EGTIC para sensibilizar para a iniciativa, as suas motivações e objetivos, a todas as partes interessadas;

	9. Eliminar qualquer falso sinal de segurança ou complacência, destacando por exemplo conformidades ou exceções; 10. Instigar o nível de urgência apropriado, dependendo da prioridade e do impacto da mudança.
Gestão do Programa	Iniciar o programa: 1. Fornecer a orientação estratégica e objetivos de alto nível, em acordo com a comissão de EGTIC; 2. Definir e atribuir papéis e responsabilidades de alto nível na iniciativa, indo deste o patrocínio do executivo ao gestor do programa e todas as partes interessadas importantes; 3. Desenvolver um esboço da justificação estratégica, indicando os fatores de sucesso permitindo a monitorização do desempenho e relatório do sucesso da melhoria na governação; 4. Obter o apoio do executivo.

Tabela 3 - Descrição da Fase 1 - O que nos Move?, obtido de [4]

Então os *inputs* indicados como necessários são [4]:

- Políticas Organizacionais, estratégias, planos de governação e de negócio e relatórios de auditorias. Para este trabalho foram consultados vários documentos, contudo devemos destacar o documento sobre as orientações estratégicas do município, o regulamento orgânico [39] depois alterado em Setembro, o plano global estratégicos de racionalização das TIC [34], auditoria IT, elaborado por uma consultora externa BDO[9] [40];
- Outras iniciativas existentes com as quais poderiam haver dependências ou impactos. Neste ponto destaca-se a dependência com a ISO 9001, onde existem alguns procedimentos TIC já definidos e podem ser consultados no processo de gestão da qualidade do município;
- Relatórios sobre a gestão das TIC, estatísticas do *HelpDesk*, questionários aos utilizadores ou outros dados indicadores de problemas nas TIC. Alguns exemplos podem ser consultados no Anexo 1 - Listagem pedidos HelpDesk 2012;
- Estudos de caso e histórias de sucesso, análises relevantes sobre GTIC. Exemplos destes estudos já foram apresentados na seção 2.2.1 e outros trabalhos consultados, sendo de grande relevância a dissertação de mestrado de Emile Kaselowski [41];
- Requisitos específicos dos utilizadores/munícipes, estratégias de marketing e prestação de serviços, posição de mercado, declarações da visão e missão em análise no documento "Grandes opções do plano 2013-2016" [42]

[9] http://www.bdo.pt/

Sendo que após o devido tratamento e para continuar para a fase seguinte será necessário obter os seguintes outputs [4]:

- Esboço da justificação estratégica que se encontra no Apêndice 2 - Justificação_Estratégica_EGTIC_Draft_v1 e que serviu de base para este documento;
- Papéis e responsabilidades de alto nível estabelecidas que se encontra em Apêndice 3 - Papéis e Responsabilidades;
- Mapa de partes interessadas identificado, suporte e envolvimento, influência e impacto, reconhecimento do esforço para lidar com a mudança, faz parte da justificação estratégica no Apêndice 2;
- Programa de chamada à intervenção (todas as partes interessadas), definido na justificação estratégica e delineado no gestor de projetos entretanto instalado e configurado (redmine[10]), Figura 16;
- Comunicação do programa de arranque (partes interessadas chave). O programa de arranque foi comunicado aos colaboradores internos das TIC, executivo, diretores e chefias, num total de quatro apresentações, Apêndice 4.1 - Apresentação_Staff_IT, Apêndice 4.2 - Apresentação Executivo, Apêndice 4.3 - Apresentação_Direção e Apêndice 4.4 - Apresentação_Novo_Executivo.

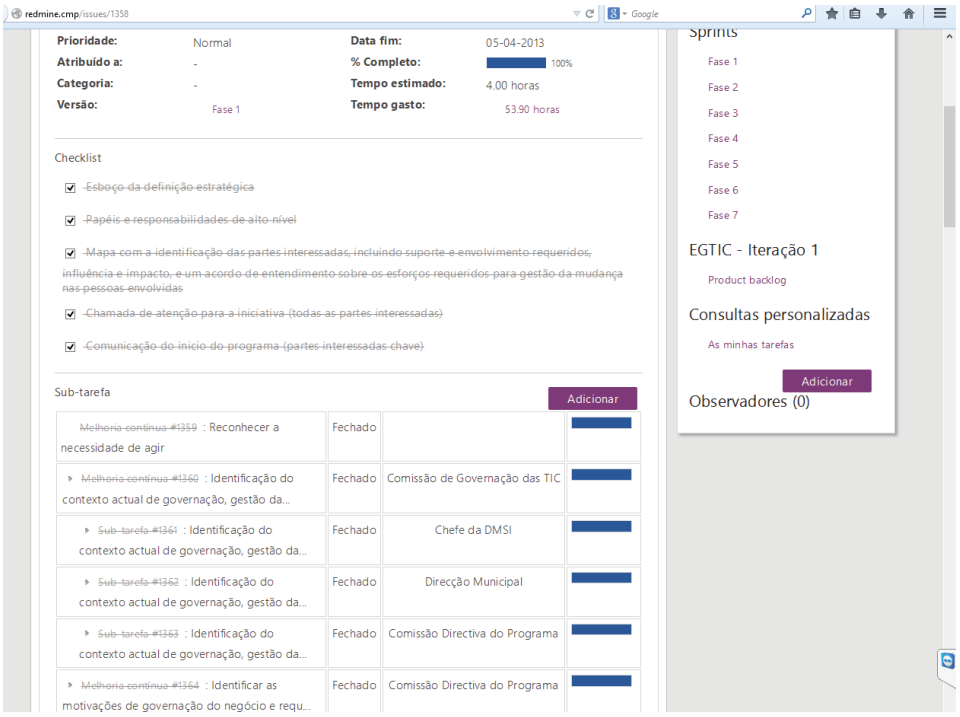


Figura 16 - Gestão de Projetos - Redmine

[10] Aplicação Web para gestão de projetos, http://www.redmine.org/

Seguindo então o estabelecido no ciclo de vida da implementação, cada fase é dividida em três conjuntos de tarefas referentes a cada um dos três componentes.

Desafios Estratégicos

Neste ponto são analisados desafios reais no caso de estudo levado a cabo no desenvolvimento desta dissertação. Esta análise inicial levanta questões de melhoria e problemas além dos apontados como objetos passíveis de resolução na solução proposta, e abre a porta para o desenho e desenvolvimento da solução.

Análise à possível implementação

Devido à natureza omnipresente das TIC e ao ritmo atual na mudança da tecnologia, é necessária uma estrutura confiável e capaz de controlar adequadamente todo o ambiente das TIC evitando diferenças de controlo e processos que exponham o município a riscos inaceitáveis.

A intenção não será a de impedir ou restringir a operacionalidade das TIC no município. Ao invés disso, pretende-se melhorar o perfil de risco de uma forma que faça sentido para os seus serviços, com ganhos em qualidade e eficiência, no cumprimento explícito dos objetivos/metas estabelecidos pela governação e gestão municipais e dos demais requisitos como os legislativos, regulamentares e/ou contratuais.

Pretende-se que a implementação desta nova estrutura seja vista, não como uma rutura com o atual modelo de governação/gestão das TIC, mas sim como uma evolução na continuidade, envolvendo de forma participada todos os interessados.

A experiência mostra que, independentemente da dimensão da iniciativa para a implementação de uma EGTIC, é essencial o executivo estar envolvido desde o início e ser ele a conduzir os esforços necessários à criação da estrutura de governação apropriada [4]. Dado que as atividades iniciais habitualmente incluem o levantamento e análise das práticas correntes, assim como, o desenho de novas estruturas, tal pode levar à necessidade de reorganização quer da estrutura base do município em relação às TIC, como das funções das TIC e a sua relação com as restantes unidades orgânicas.

O executivo deverá nomear responsáveis com papéis bem definidos na direção/coordenação do programa de implementação da EGTIC.

São muitos os fatores que indiciam a necessidade de revisão ou criação de novas práticas na governação das TIC. O reconhecimento da existência de pontos que

podem ser alvo de melhorias e alterações no ambiente interno e externo da organização são utilizados como fatores impulsionadores desta iniciativa de implementação de uma EGTIC, razão pela qual são descritos de seguida.

Pontos a melhorar

Após uma análise ao estado atual dos SI e TIC assim como aos procedimentos existentes na sua gestão, foram identificados alguns pontos críticos "*pain points*" que deverão ser analisados e levados em conta para a escolha dos processos a capacitar. Esta análise foi realizada usando os dados de auditorias, entrevistas e da real perceção do estado financeiro e de recursos na autarquia recolhidos antes do início deste trabalho e durante o mesmo.

a) Alinhar as TIC e os SI aos objetivos da autarquia (ex. Redução de custos);
b) Analisar iniciativas que ainda não criam valor público suficiente (ex. CRM, ERP);
c) Detetar falhas de *hardware* que provocam constrangimentos no atendimento ao munícipe (ex. *DataStorage*, *Datacenter*, Impressoras);
d) Criar SLA para todos os fornecedores/prestadores de serviços na área das TIC (ex. "fornecedor do ERP");
e) Analisar a quantidade e qualidade de fornecedores e prestadores de serviços externos (ex. o procedimento de redução dos vários fornecedores de impressão dificultam a gestão dos ativos);
f) Criar políticas e procedimentos oficialmente reconhecidos (ex. Segurança na utilização dos meios, correta utilização do correio institucional);
g) Flexibilizar a solução de ERP para permitir a inovação (ex. criação de *webservices* para permitir a interoperabilidade com outras aplicações);
h) Maior envolvimento das TI no planeamento estratégico do município (ex. identificação de tecnologias inovadoras na redução de alguns tipos de custo);
i) Criar a função auditoria nos sistemas de informação (ex. auditorias internas periódicas para identificação de falhas e correções no funcionamento dos SI);
j) Transparência de custos e custos de TIC "escondidos" (ex. consumo energético dos *Datacenters*);
k) Criar um "portefólio" de serviços TI (ex. Identificar os serviços que são prestados, aqueles que deixam de ser prestados e aqueles que se encontram em fase de desenvolvimento);
l) Criar procedimentos uniformizados de *servicedesk* otimizando os recursos existentes (ex. O *servicedesk* não é utilizado de forma uniforme por toda a estrutura da autarquia, havendo descentralização na distribuição de tickets);

m) Formação específica dos técnicos de informática e formação nas TIC dos demais colaboradores (ex. constantes telefonemas com questões que deveriam ser básicas na utilização dos meios de TIC);
n) Modernizar os recursos de *hardware* críticos (ex. implementação de sistemas de redundância e suporte nos servidores);
o) Melhorar as instalações físicas do *Datacenter* (ex. melhorar as condições de segurança, designadamente os acessos físicos?);
p) Criar procedimentos uniformes de gestão de projetos, alterações e configurações (ex. não existe uniformização aplicacional na gestão de projetos, inexistência de uma CMDB (*Configuration Management Database*);
q) Organizar a infraestrutura (ex. cablagens, serviços e aplicações descentralizados);
r) Criar ferramentas de apoio à decisão (ex. *Datamining* do ERP na elaboração de tabelas e gráficos pré-estabelecidos de KPI (*Key Performance Indicators*));
s) Incrementar os serviços *on-line* ao Munícipe (ex. possibilidade de relatar problemas existentes nos espaços públicos de forma remota; criação do portal da cidade – viragem ao exterior);
t) Existência de vários domínios "*untrusted*" com impacto na gestão de identidades (ex. vários domínios em espaços diferentes ligados fisicamente por fibra mas separados logicamente em termos de confiança);
u) Conversações em *trunk* para locais (ex. Teatro, Museu, GSM);
v) Implementar um sistema de monitorização de serviços/equipamentos em tempo real e das suas dependências (ex. existência de sistema de alertas SMS para os técnicos na falha de serviços críticos);
w) Esforços complicados de garantia das TIC devido à natureza do negócio de alguns serviços (ex. obrigatoriedades legais de registos físicos).

Acontecimentos internos e externos

Além dos pontos a melhorar identificados no ponto anterior e que dizem respeito aos pontos críticos identificados após uma auditoria e entrevistas com as partes interessadas, existem acontecimentos que também alavancam esta iniciativa de melhoria.

a) A recessão económica no país e reciprocamente nos municípios, obrigam atualmente a uma forte contenção nos custos das suas operacionalidades. Esse esforço exige que haja uma revisão nos mecanismos de governação das TIC de modo a permitir uma otimização de custos em larga escala, uma

melhoria na performance dos serviços atualmente prestados ou ainda a criação de novos serviços com base em novos paradigmas;

b) As alterações nas estruturas organizacionais dos municípios com a definição de novas UEN (Unidades Estratégicas de Negócio), extinção de departamentos e fusão de unidades orgânicas, com a consequente alteração dos fluxos de trabalho;

c) Alterações e evoluções tecnológicas significativas, tais como a alteração atual de paradigma de computação de ambiente cliente-servidor, com a proliferação da computação em *cloud*, da virtualização e dispositivos móveis, obrigam a que, necessariamente e acreditando que existe o dever de prestar o melhor serviço possível, sejam realizadas alterações na forma como a infraestrutura e aplicações são desenvolvidas, adquiridas e colocadas em produção;

d) Uma governação baseada em projetos e numa constante tentativa de aproximação ao munícipe, leva a que se tratando de informação, tenha influência no funcionamento da EGTIC. Por forma a dinamizar e não entravar projetos e comunicações, a EGTIC deverá poder tomar decisões da forma mais célere possível, pelo que deverá ter maior liberdade para isso, ou estar mais perto do decisor final;

e) A legislação e regulamentos obrigam a um repensar e a reestruturar a forma da atual governação e gestão das TIC, de modo a ser mais eficiente, a cumprir e manter os processos e práticas de acordo com o permitido, inclusive a ter em atenção a questão da privacidade da informação causada com a omnipresença das TIC. Da necessidade do município obter novos tipos de relatórios e informações à modernização administrativa:

    - Lei n.º 109/2009, de 15 de Setembro – LEI DO CIBERCRIME;
    - DL n.º 7/2004, de 07 de Janeiro – COMERCIO ELETRONICO NO MERCADO INTERNO E TRATAMENTO DE DADOS PESSOAIS;
    - DL n.º 123/2009, de 21 de Maio - CONSTRUÇÃO, ACESSO E INSTALAÇÃO DE REDES;
    - Lei n.º 67/98, de 26 de Outubro – LEI DA PROTECÇÃO DE DADOS PESSOAIS;
    - Lei n.º 42/2013, de 03 de Julho - LEI DAS COMUNICAÇÕES ELECTRÓNICAS;
    - Lei n.º 46/2012, de 29 de Agosto - PROTECÇÃO DE DADOS PESSOAIS E PRIVACIDADE NAS TELECOMUNICAÇÕES;
    - DL n.º 122/2000, de 04 de Julho - PROTECÇÃO JURÍDICA DAS BASES DE DADOS;

- DL n.º 334/97, de 27 de Novembro - PROTECÇÃO JURÍDICA DE PROGRAMAS DE COMPUTADOR;
- Resol. n.º 91/2009, de 15 de Setembro - PROTOCOLO ADICIONAL À CONVENÇÃO SOBRE O CIBERCRIME;
- DL n.º 107/2012, de 7 de fevereiro – REGULA O DEVER DE INFORMAÇÃO E A EMISSÃO DE PARECER PRÉVIO RELATIVOS À AQUISIÇÃO DE BENS E À PRESTAÇÃO DE SERVIÇOS NO DOMINIO DAS TECNOLOGIAS DE INFORMAÇÃO E COMUNICAÇÃO;
- Resolução Lei n.º 36/2011, de 21 de Junho – ADOÇÃO DE NORMAS ABERTAS NOS SISTEMAS INFORMÁTICOS DO ESTADO;
- RCM 48/2012 de 21 de maio – DETERMINA OS SISTEMAS CRÍTICOS, REFERIDOS NO DL 107/2012;
- RCM n.º 91/2012, de 8 de Novembro – REGULAMENTO NACIONAL DE INTEROPERABILIDADE DIGITAL;
- Lei n.º 49/2012, de 29 de Agosto - ESTATUTO DO PESSOAL DIRIGENTE DAS CÂMARAS MUNICIPAIS;
- Lei n.º 27/96, de 01 de Agosto – LEI DA TUTELA ADMINISTRATIVA;
- Lei n.º 73/2013, de 03 de Setembro - REGIME FINANCEIRO DAS AUTARQUIAS LOCAIS E ENTIDADES INTERMUNICIPAIS;
- Lei n.º 22/2012, de 30 de Maio - REGIME JURÍDICO DA REORGANIZAÇÃO ADMINISTRATIVA TERRITORIAL AUTÁRQUICA;
- Lei n.º 75/2013, de 12 de Setembro - REGIME JURÍDICO DAS AUTARQUIAS LOCAIS;
- DL n.º 442/91, de 15 de Novembro - CÓDIGO DO PROCEDIMENTO ADMINISTRATIVO;
- DL n.º 18/2008, de 29 de Janeiro - CÓDIGO DOS CONTRATOS PÚBLICOS (CCP);
- Lei n.º 58/2008, de 09 de Setembro - ESTATUTO DISCIPLINAR DOS TRABALHADORES QUE EXERCEM FUNÇÕES PÚBLICAS;
- Lei n.º 4/2004, de 15 de Janeiro - PRINCÍPIOS E NORMAS A QUE OBEDECE A ORGANIZAÇÃO DA ADMINISTRAÇÃO DIRECTA DO ESTADO;
- DL n.º 92/2010, de 26 de Julho - PRINCÍPIOS E REGRAS PARA SIMPLIFICAR O LIVRE ACESSO E EXERCÍCIO DAS ACTIVIDADES DE SERVIÇOS;
- Lei n.º 59/2008, de 11 de Setembro - REGIME E REGULAMENTO DO CONTRATO DE TRABALHO EM FUNÇÕES PÚBLICAS;

- Lei n.º 67/2007, de 31 de Dezembro - REGIME DA RESPONSABILIDADE CIVIL EXTRACONTRATUAL DO ESTADO;
- Lei n.º 12-A/2008, de 27 de Fevereiro - REGIMES DE VINCULAÇÃO, DE CARREIRAS E DE REMUNERAÇÕES - FUNÇÕES PÚBLICAS;
- Lei n.º 57/2011, de 28 de Novembro - SISTEMA DE INFORMAÇÃO DA ORGANIZAÇÃO DO ESTADO (SIOE);
- Lei n.º 66-B/2007, de 28 de Dezembro - SISTEMA INTEGRADO DE GESTÃO E AVALIAÇÃO DO DESEMPENHO NA ADMINISTRAÇÃO PÚBLICA – SIADAP;

f) A segurança em sistemas de informação é cada vez mais uma obrigação. A inexistência de processos e controlos de segurança efetivos colocam em risco a operacionalidade e a imagem do município. Existe a necessidade de um mecanismo eficaz para a criação de um sistema de gestão da segurança da informação e TIC;
g) Desejo de melhorar significativamente o valor obtido dos investimentos nas TIC melhorando os serviços através da inovação, otimização de meios e criação de novas oportunidades e serviços;
h) Necessidade de alinhamento com a Agenda Portugal Digital publicada em Diário da República, 1.ª Série n.º 252 – 31 Dezembro de 2012 a resolução do Conselho de Ministros n.º 112/2012.

Observações efetuadas no decorrer da fase 1

No contexto atual a governação é efetuada em reuniões entre o chefe da Divisão, "gestores" TIC e o vereador do pelouro. Em âmbito geral o modelo de governação é o modelo da autarquia, não havendo um especifico para as tomadas de decisão respeitantes às TIC.

Principais opções de negócio para 2013-2016:

- Equilibrar as contas municipais;
- Dinamizar a economia local;
- Garantir a operacionalidade dos equipamentos municipais;
- Garantir as funções básicas municipais.

Projetos em curso nas TIC:

- Aquisição de *softwares* específicos para gestão documental com pareceres técnicos e análise automática de revisões;
- Analisar as renovações ou não de alguns licenciamentos de *software*;

- Resolver problemas contratuais com alguns fornecedores do qual dependem alguns serviços tais como o SIG ou alojamento do portal institucional;
- Elaboração de um novo portal para o município.

Projetos em curso no município

- Reestruturação da orgânica do município;
- Redução de custos com serviços e aquisições.

A certificação da ISO 9001 é levada como uma mudança em curso nos processos representativos da área das TIC.

O ambiente atual é um ambiente de mudança a todo o nível no município, o que poderá ser um facilitador da mudança a utilizar. A cultura existente poderá ser um entrave devido à conhecida resiliência à mudança. Deverão ser alavancadas as relações não formais para comunicação e informação de mudanças, ao mesmo tempo que são implementadas formas formais e intrínsecas ao município na comunicação da mesma.

Nesta primeira fase o impacto da mudança deverá ser maior e mais visível internamente à DMSI devido a previsíveis alterações à forma de funcionar. A mudança de um sistema de gestão para um sistema de governação/gestão com a inclusão de elementos externos às TIC na tomada de decisão, terá impacto na disponibilidade dos meios diferenciados entre suporte e serviços.

Após consulta com a chefia da DMSI e a vereação responsável, apesar do reconhecido risco devido às eleições de Outubro de 2013 (a decorrerem no meio do programa), optou-se por dar inicio aos esforços de implementação.

Nesta iteração, fase 1, não é possível identificar conformidades para exemplificar figuras de exceção que possam indicar falsos sinais de segurança.

Foi transmitida superiormente o entendimento sobre a necessidade de agir, tendo sido demonstrado na justificação estratégica, Apêndice 2 - Justificação_Estratégica_EGTIC_Draft_v1, a urgência em dar inicio ao desenvolvimento do programa de implementação. Como já identificado, o executivo irá mudar nas próximas eleições, sendo urgente o planeamento e operacionalidade do novo sistema até à entrada do mesmo. Foi então concedido de forma oficial à equipa de implementação do programa a autorização para prossecução dos trabalhos, Apêndice 5 - Autorização Superior para prosseguir com o programa de implementação.

4.3.2. Onde nos encontramos?

Terminada a fase 1 até ao nível onde foi possível aprofundar, com os dados existentes e demonstrado o valor às partes interessadas e identificadas, é obtida a autorização e apoio para avançar para a fase seguinte que determina o estado atual. O estado atual é determinado fazendo uso dos resultados obtidos na fase anterior, designadamente as questões chave (pontos a melhorar e acontecimentos internos e externos). Novamente com o apoio do guia de implementação do CobiT 5 [4] identificam-se tarefas, *inputs* e *outputs* nesta fase.

Tipo de Tarefa	**Tarefas**
Melhoria Contínua	Avaliar o estado atual: 1. Identificar objetivos chave da autarquia e o respetivo suporte das TIC; 2. Estabelecer o significado e natureza da contribuição das TIC (soluções e serviços), necessários para suportar os objetivos do município; 3. Identificar questões e fraquezas chave de governação, relacionadas com soluções e serviços atuais e futuros, qual a arquitetura empresarial necessária para suportar os objetivos das TIC e quaisquer restrições ou limitações; 4. Avaliar o benefício/valor na capacitação do risco (*benefit/value enablement risk*), avaliação do risco na operacionalidade das TIC/prestação de serviços e conclusão de iniciativas/projetos relacionados com processos críticos das TIC; 5. Identificar e selecionar processos TIC críticos para garantir que o risco é mitigado; 6. Perceber a posição de aceitação de risco tal como definido pelo executivo/diretores/chefias.
Facilitador da Mudança	Definir problemas e oportunidades: 1. Reunir uma equipa nuclear das TIC e envolvendo elementos não TIC, com o conhecimento/perícia/perfil/experiência/credibilidade e autoridade apropriadas para conduzir a iniciativa; 2. Identificar e gerir interesses instalados que possam existir dentro da equipa, para assim criar o necessário nível de confiança; 3. Criar o ambiente apropriado para um trabalho em equipa ótimo; 4. Realizar um *workshop* para criar consenso (visão partilhada) dentro da equipa e adotar um mandato para a iniciativa de mudança; 5. Identificar os agentes da mudança com os quais o núcleo da equipa pode trabalhar, usando o princípio de apoio em cascata, para garantir o apoio alargado das partes interessadas durante cada fase do ciclo de vida; 6. Documentar as forças identificadas durante a avaliação do estado atual que possam ser usadas como elementos positivos em comunicações, bem como em potenciais ganhos rápidos que possam ser alavancados da perspetiva de facilitação da mudança.

Gestão do Programa	Iniciar o programa: 1. Rever e avaliar o esboço da justificação estratégica, a viabilidade da iniciativa e o potencial ROI; 2. Atribuir papéis, responsabilidades e proprietários dos processos e assegurar o empenhamento e suporte das partes interessadas afetadas na definição e execução da iniciativa; 3. Identificar desafios e fatores de sucesso.

Tabela 4 - Descrição da Fase 2 - Onde nos encontramos?, obtido de [4]

Então os *inputs* indicados como necessários são [4]:

- Todos os outputs da fase anterior;
- Planos e estratégias da autarquia e das TIC. Estes documentos já foram usados na fase 1 [42] [38], sendo que nesta fase a sua análise incidiu na perspetiva de auditoria ao funcionamento das TIC;
- Processos, políticas, normas, procedimentos e especificações técnicas das TIC. Aqui foi usada toda a documentação resultante do sistema de gestão da qualidade certificado na autarquia (ISO 9001);
- Perceção dos processos de negócio e da contribuição das TIC. Da mesma forma que para os processos TIC se analisou a documentação da ISO 9001 existente, também aqui se procuraram os processos nesta certificação descritos. No entanto, identificaram-se grandes problemas na generalização e implementação dos mesmos;
- Relatórios de auditoria, políticas de gestão de risco, relatórios da performance das TIC. Os mesmos documentos já indicados na fase anterior. Foi efetuada uma auditoria aos processos existentes utilizando ferramentas do CobiT 5, e adaptação das folhas de cálculo com as fórmulas de análise para capacitação segundo a ISO 15504. O resultado desta atividade está registado no Apêndice 16 - Entendimento sobre o estado atual dos procedimentos selecionados;
- Planos de continuidade de negócio, análises de impacto, requisitos legais, arquitetura empresarial, SLA's, níveis de acordo operacional. Neste ponto percebeu-se que como apologiza o Prof. Doutor José Tribolet [43], a tarefa não será fácil por não se encontrar definida de forma clara, descritiva e atualizada a arquitetura empresarial do município em relação aos serviços, transações e atores;
- Portefólio de investimentos e projetos, planos de projetos e iniciativas, metodologias de gestão de projetos, relatórios de projeto. Foi feito um levantamento de projetos e do seu estado atual, ver Apêndice 6 - Portefólio de projetos e iniciativas.

Sendo que após o devido tratamento e para continuar para a fase seguinte será necessário obter os seguintes outputs [4]:

- Os objetivos da autarquia para as TIC e o seu impacto nas TIC. Estes podem ser consultados no Apêndice 7 - Mapeamento objetivos do Município com objetivos TIC relacionados com os do Município;
- Entendimento do risco e impacto resultante do não alinhamento dos objetivos das TIC e falhas na prestação de serviços e projetos, ver Apêndice 8 - Cenário de Riscos e Capacidade dos Processos;
- Processos selecionados e objetivos, encontrados fazendo uso do encadeamento de objetivos idealizado pelo CobiT 5, Figura 6, ver Apêndice 9 - Metas-Objetivos de Capacidade para os Processos Selecionados;
- Classificação da capacidade atual dos processos selecionados, Apêndice 1 - Análise de Capacidade;
- Avaliação do esboço da justificação estratégica, ver Apêndice 10 - Justificação_Estratégica_EGTIC_Draft_v2.

Observações efetuadas no decorrer da fase 2

A autarquia define áreas estratégicas onde necessita do apoio das TIC no art. º 18 alínea c) do novo regulamento orgânico [38]:

- Atendimento e relação com o munícipe;
- Modernização administrativa;
- Envolvimento do cidadão;
- Transparência.

A identificação de algumas questões e fraquezas chave de governação relacionadas com os atuais ou futuros serviços:

- Ausência de uma estrutura de governação das TIC;
- Proliferação de bases de dados;
- Chamadas para números diretos de suporte das TIC (prática que vai contra as melhores práticas da industria para a prestação de serviços de suporte);
- Ausência de uma gestão de projetos conforme definido pelos *standards* da indústria;
- Inflexibilidade do sistema da arquitetura aplicacional;
- Restrições orçamentais derivadas da situação económica do município.

No Apêndice 11 - Mapeamento das questões chave com os objetivos TIC relacionados com os objetivos do Município são enquadrados com os processos identificados no

CobiT 5 [10], Apêndice 12 - Mapeamento das questões com os processos CobiT 5 e que deverão ser implementados para suprimir as necessidades identificadas.

O CobiT 5 recomenda à partida a definição de alguns processos que deverão ser implementados desde o início da implementação do programa, sendo eles:

- Alinhar, Planear e Organizar:
    - APO01 (Gerir a Framework de gestão das TIC);
    - APO02 (Definir a estratégia);
    - APO05 (Gerir o portefólio);
    - APO12 (Gerir o risco).
- Construir, Adquirir e Implementar:
    - BAI01 (Gerir Programas e projetos).
- Monitorizar, Avaliar e Analisar:
    - MEA01 (Monitorizar e avaliar performance e conformidade);
    - MEA02 (Monitorizar o sistema de controlo interno);
    - MEA03 (Monitorizar e avaliar conformidades com requisitos externos).

Com base na prioridade definida para a criação de procedimentos através da análise dos pontos críticos foram identificados os seguintes:

- APO03 (Gerir a Arquitetura empresarial);
- APO06 (Gerir orçamentos e custos);
- APO07 (Gerir Recursos Humanos);
- APO10 (Gerir Fornecedores);
- APO11 (Gerir Qualidade);
- APO13 (Gerir Segurança);
- BAI04 (Gerir capacidade e disponibilidade);
- BAI06 (Gerir Alterações);
- BAI09 (Gerir Ativos);
- BAI10 (Gerir Configurações);
- Todos os processos de Governação;
- Todos os processos de Prestação de Serviços e Suporte.

Como primeiro resultado e com a concordância dos elementos envolventes, determinou-se que a necessidade atual de processos críticos em falha será toda a área de prestação de serviços e suporte. Estes processos foram também priorizados devido à necessidade de libertar recursos humanos para a capacitação dos outros processos. Como identificado no Apêndice 1 - Análise de Capacidade, alguns dos

processos da Prestação de Serviços e Suporte possuem algum nível de capacidade, o que a sua escolha para capacitação poderá significar ganhos rápidos.

Não foi efetuada análise de risco nesta fase nem foi identificada a apetência da autarquia ao risco. Encontra-se em estudo por parte da DMSI uma possível *framework* para análise de risco.

Para garantir que o risco é identificado e mitigado foram identificados os seguintes processos críticos:

- APO12 (Gerir o Risco);
- APO13 (Gerir Segurança).

Não existe por parte das chefias uma posição sobre a aceitação do risco. Existe a noção do executivo sobre a necessidade de um plano de contingência, não sendo no entanto formal a aceitação do risco a falhas na segurança física e lógica que justifiquem a existência do mesmo.

A política de segurança da informação foi enviada para aprovação, não havendo até ao momento autorização para colocar em vigor e divulgar.

A equipa nuclear nesta fase é constituída por dois elementos:

- Pedro Santos;
- Humberto Chula;
- Nuno Gouveia.

As questões inerentes levantadas com a necessidade de conhecimentos fora das TIC têm sido esclarecidas recorrendo diretamente aos colaboradores da autarquia responsáveis pelas áreas. Toda a DMSI está no entanto envolvida.

Foram criados grupos de interessados:

- Gestores TIC;
- Proprietários de Processos;
- CIO;
- Divisão Jurídica (risco e conformidade);
- Auditores TIC.

Para criar um ambiente de trabalho para o desenvolvimento do programa, foi criado um laboratório de testes e segurança dos sistemas de informação e comunicação, alocados recursos humanos a tempo inteiro para a análise do CobiT 5 e adaptação

do sistema. Foram também disponibilizados meios físicos e lógicos dentro dos existentes na DMSI para a persecução das necessidades do trabalho em equipa.

Foram identificadas as seguintes forças que podem ser usadas como elementos positivos a comunicar, assim como em ganhos rápidos que possam ser alavancados na perspetiva de facilitar a mudança:

- Reestruturação em curso da orgânica do município;
- Necessidade de redução de custos;
- Projeto Portugal Digital[11] [44];
- Reestruturação das TIC na administração pública [34];
- Apoio da chefia da DMSI para a mudança;
- A existência de um *ServiceDesk* em funcionamento;
- Apoio e envolvimento dos elementos da DMSI;
- Ganhos rápidos:
    - Libertação de Recursos (RH e Ativos) para melhoria/inovação e modernização dos serviços e sistemas com a otimização do *servicedesk*.

4.3.3. Onde queremos chegar?

Terminada a fase 2 é obtida a autorização e apoio para avançar para a fase seguinte que identifica onde queremos chegar. O onde queremos chegar é determinado fazendo uso dos resultados obtidos na fase anterior, e tem como objetivos: i) determinar a capacidade a atingir para cada um dos processos selecionados. ii) determinar as diferenças entre o que existe e o que deveria existir em cada um dos processos selecionados. iii) traduzir essas diferenças em oportunidades de melhoria, iv) utilizar esta informação para criar uma justificação estratégica e um plano de alto nível para a iniciativa. Novamente com o apoio do guia de implementação do CobiT 5 [4] identificam-se tarefas, *inputs* e *outputs* nesta fase.

Tipo de Tarefa	**Tarefas**
Melhoria Contínua	Definir o estado a alcançar e analisar falhas: 1. Definir objetivos de melhoria: a. Baseados nas necessidades de desempenho e conformidade da autarquia, decidir os objetivos iniciais e ideais de níveis de capacidade de cada processo no curto e médio prazo; b. Na medida do possível, comparar com referências internas, para identificar melhores práticas que possam ser adotadas;

[11] http://www.ei.gov.pt/iniciativas/detalhes.php?id=29

	c. Na medida do possível, comparar com referências externas (outras autarquias), para ajudar a decidir na escolha do nível de capacidade desejada; d. Avaliar a razoabilidade dos níveis desejados (individualmente e como um todo) tentando verificar o que é alcançável e desejável, e que pode ter um maios impacto positivo dentro de um espaço de tempo determinado. 2. Analisar falhas: a. Utilizar o conhecimento das capacidades atuais (por atributo) e compara-las aos níveis desejados de capacidade; b. Alavancar as forças existentes, tanto quanto possível, para lidar com as falhas e procurar orientação nas boas práticas (Cobit, ITIL, TOGAF, ISO...) para colmatar outras falhas; c. Procurar por padrões que indiquem causas raiz para serem resolvidas. 3. Identificar potenciais melhorias: a. Transformar falhas em potenciais melhorias; b. Identificar o risco não mitigado, residual, e assegurar formalidade na sua aceitação.
Facilitador da Mudança	Descrever e comunicar os resultados desejados: 1. Descrever o plano de alto nível facilitador de mudança e os objetivos baseados nas tarefas facilitadoras de mudança a desenvolver; 2. Desenvolver uma estratégia de comunicação para otimizar a sensibilização e o apoio; 3. Garantir a vontade de participar (*picture of the change*); 4. Articular a base lógica para, e benefícios de, efetuar a mudança para suportar a visão e descrever os impactos de não se efetuar a mudança (*purpose of the change*); 5. Fazer a ligação com os objetivos da iniciativa nas comunicações e demonstrar como a mudança irá trazer benefício; 6. Descrever um *roadmap* de alto nível para se alcançar a visão (plano para a mudança), bem como o envolvimento necessário dos vários interessados (papeis na mudança); 7. Utilizar o executivo para fazer declarações chave para dar o mote de suporte na implementação; 8. Utilizar agentes de mudança para comunicação informal adicionalmente às comunicações formais; 9. Comunicar pela ação - a equipa guia, deve dar o exemplo; 10. Apelar às suas emoções quando necessário, para levar as pessoas a alterar comportamentos; 11. Capturar o feedback inicial da comunicação (reações e sugestões) e adaptar a estratégia de comunicação em conformidade.
Gestão do Programa	Definir um *roadmap*:

	1. Definir a orientação da iniciativa, âmbito, benefícios e objetivos de alto nível; 2. Assegurar o alinhamento dos objetivos com o negócio e estratégias TIC; 3. Considerar o risco e ajustar o âmbito em conformidade; 4. Considerar as implicações da facilitação da mudança; 5. Obter orçamentos necessários e definir responsabilizados e responsabilidades pela iniciativa; 6. Criar e avaliar uma justificação estratégica detalhada, orçamento, prazos e um plano e alto nível para a iniciativa.

Tabela 5 - Descrição da Fase 3 - Onde queremos chegar?, obtido de [4]

Então os *inputs* indicados como necessários são [4]:

- Todos os outputs da fase anterior;
- Parâmetros de referência das capacidades internas e externas. Os parâmetros utilizados foram a quantidade de registos efetuado no atual sistema de *HelpDesk*, Anexo 1 - Listagem pedidos HelpDesk 2012 e em conversas tidas com os atuais técnicos sobre a adoção dos procedimentos determinados para as TIC na ISO 9001;
- Boas práticas (Cobit, ITIL), normas (ISOs) e outras referências (*case studies*, estudos, *papers*), foram analisados conforme indicado no capítulo 2 desta dissertação;
- Análise das partes interessadas, esta análise resume-se ao *feedback* das apresentações efetuadas assim como dos *workshops* realizados com os técnicos da DMSI.

Sendo que após o devido tratamento e para continuar para a fase seguinte será necessário obter os seguintes outputs [4]:

- Classificação da capacidade desejada para os processos selecionados. Depois das determinações e achados resolvidos na fase anterior, chegou-se à conclusão de capacitação indicada no Apêndice 9 - Metas-Objetivos de Capacidade para os Processos Selecionados;
- Descrição de oportunidades de melhoria, no processo escolhido para capacitar identificam-se no Anexo 2 - Oportunidade Melhoria DSS02 - Gerir Pedidos de Serviço e Incidentes;
- Documento de resposta ao risco, incluindo o risco não mitigado, sendo que como esclarecido na fase anterior, não foi efetuada nenhuma análise concreta ao risco, pelo que o único documento de análise de risco existente é o Apêndice 8 - Cenário de Riscos e Capacidade dos Processos;

- Estratégia de comunicação e comunicação da visão de mudança, cobrindo os 4 p (*picture, purpose, plan, part*):
    - *Purpose - Describe why you are making the change*
    - *Picture - Describe what the future will look like*
    - *Plan - Describe the steps you need to take to get there*
    - *Part - Describe the part you need the specific employee to play; specify your requests*
- Justificação estratégica detalhada. As justificações para cada projeto passarão a recorrer a um *template* padrão Apêndice 13 - Modelo do Documento de Justificação Estratégica para Projetos TIC, assim pretende-se uniformizar para melhor comparar e priorizar;
- Plano de alto nível da iniciativa e métricas chave que serão usadas para efetuar a monitorização da iniciativa e do desempenho operacional. Seguindo o próprio CobiT 5, Anexo 3 - DSS02 - Gerir pedidos de serviço e incidentes;

Observações efetuadas no decorrer da fase 3

Apesar da vontade de capacitar todos os processos, o desejo deve ser travado com a ambição de que o ciclo de melhoria seja contínuo, devendo ser dada prioridade aos processos que tragam ganhos rápidos, assim como aqueles que já possuam algum nível de capacidade.

Levar em conta que ao se escolher um determinado processo para capacitar, este possui dependência de determinados *outputs* de outros processos que possam não existir, ou ter a competência para os fornecer. Tais *outputs* são identificados para ou se criarem, ou efetuar de alguma forma esse preenchimento, Apêndice 14 - Listagem pré-requisitos para o DSS02. Assim durante a capacitação do mesmo, os *inputs* necessários serão gerados, o que vai de certa forma promover a capacitação de outros processos.

4.3.4. O que é necessário fazer?

Nesta fase é exigível o planeamento de soluções que permitam alcançar o identificado na fase anterior. É importante a utilização da já identificada justificação estratégica para cada projeto de melhoria ou capacitação. De igual forma ao efetuado nas fases anteriores, foi seguido o guia de implementação do CobiT 5 [4] dentro daquilo que é possível na realidade encontrada.

Tipo de Tarefa	**Tarefas**
Melhoria Contínua	Desenhar e construir melhorias:

	1. Para cada melhoria considerar o benefício potencial e facilidade de implementação (Custo, Esforço, Sustentabilidade); 2. Organizar as melhorias numa grelha de oportunidades para identificar ações prioritárias (baseado no beneficio e facilidade de implementação); 3. Focagem nas alternativas que mostrem maior benefício/maior facilidade de implementação; 4. Considerar quaisquer outras ações de mostrem alto benefício/maior dificuldade de implementação para possível decomposição (decompor em melhorias mais pequenas e avaliar os benefícios e facilidade de implementação); 5. Priorizar e selecionar melhorias; 6. Analisar as melhorias selecionadas com os requisitos de detalhe para uma definição de alto nível do projeto, considerando a abordagem, resultados, recursos necessários, recursos estimados, prazos estimados, dependências e risco do projeto; 7. Considerar a viabilidade, ligação com motivações iniciais de valor e risco e acordar os projetos a ser incluídos na justificação estratégica para aprovação; 8. Registar projetos e iniciativas não aprovadas num registo para potenciais considerações futura.
Facilitador da Mudança	Conferir poderes aos participantes e identificar os ganhos rápidos: 1. Obter apoio tentando empenhar os afetados pela mudança no desenho, através de mecanismos como *workshops* e revisão dos processos, conferindo a possibilidade de aceitar a qualidade dos resultados; 2. Desenhar planos de resposta à mudança para a gestão proactiva dos impactos da mudança, e maximizar o envolvimento durante o processo de implementação; 3. Identificar ganhos rápidos que façam prova do conceito de iniciativa de melhoria. Estas devem ser visíveis e inequívocas, criar impulso e fornecer o reforço positivo do processo; 4. Quando possível, aproveitar as forças existentes identificadas na fase 2 para obter ganhos rápidos; 5. Identificar forças em processos de negócio existentes que podem ser alavancados.
Gestão do Programa	Desenvolver um plano da iniciativa:

	1. Organizar potenciais projetos na globalidade da iniciativa, na sequência preferencial considerando atribuição para os resultados desejados, necessidades de recursos e dependências; 2. Utilizar técnicas de gestão de portefólios para assegurar que o programa está conforme com os objetivos estratégicos e as TIC possuem um conjunto equilibrado de iniciativas; 3. Identificar o impacto de iniciativas de melhoria nas TIC e na Autarquia e indicar como o impulso de melhoria deverá ser mantido; 4. Desenvolver um plano de mudança, documentando qualquer migração, conversão, teste, formação, processo ou outras atividades que devam ser incluídas na iniciativa como parte da implementação; 5. Identificar e acordar as métricas a utilizar para a medição de resultados do programa de melhoria em termos dos fatores de sucesso iniciais da iniciativa; 6. Guia para alocação e priorização dos recursos da autarquia, TIC e auditoria necessário para alcançar os objetivos da iniciativa e projetos; 7. Definir um portefólio de projetos que irão incluir os requisitos necessários do programa; 8. Definir os resultados necessários, considerando toda a abrangência das atividades requeridas para alcançar os objetivos; 9. Nomear, se requerido, comissões de implementação para projetos específicos no âmbito do programa; 10. Estabelecer planos de projeto e procedimentos de relatórios facilitadores do progresso a ser monitorizado.

Tabela 6 - Descrição da Fase 4 - O que é necessário fazer?, obtido de [4]

Então os *inputs* indicados como necessários são [4]:

- Todos os outputs da fase 3;
- Folha de cálculo com as oportunidades, melhores práticas e normas, avaliações externas e avaliações técnicas, este recurso para o caso do projeto de capacitação do DSS02 é-nos fornecido pelo próprio CobiT 5, Anexo 3 - DSS02 - Gerir pedidos de serviço e incidentes, no entanto também é utilizado de forma mais específica os *workflows* fornecidos pela ITIL;
- Forças identificadas nas fases anteriores, aqui referir a existência de processos no âmbito da ISO 9001 que poderão ser úteis no apoio à mudança devido há já existência de certa exigência de registos e procedimentos, apesar de não controlada a sua utilização.

Sendo que após o devido tratamento e para continuar para a fase seguinte será necessário obter os seguintes *outputs* [4]:

- Identificação de ganhos rápidos, no decorrer da criação da justificação estratégica para o projeto selecionado, foi identificado como ganho rápido a

adaptação da solução de *software* de gestão de pedidos de serviços e incidentes já em produção no município;

- Registos de projetos não aprovados, nesta primeira interação não são levados em conta mais projetos além do da capacitação do processo escolhido;
- Plano da iniciativa, que sequencia planos individuais com recursos alocados, prioridades e resultados. Todos os recursos da DMSI (exceto os necessários para manter a operacionalidade normal dos sistemas) são alocados à implementação e cumprimento do processo escolhido;
- Métricas de sucesso, identificadas na Justificação Estratégica.

Observações efetuadas no decorrer da fase 4

Numa questão de otimização e rapidez, passou a dedicar-se espaço ao processo DSS02, identificado como processo a capacitar, e como definido na fase anterior, foi elaborada uma justificação estratégica para o mesmo, Apêndice 15 - Justificação Estratégica - Estabelecer e fazer cumprir Processos de Service Desk.

Os *outputs* pretendidos nesta fase são na sua abrangência reconhecidos em cada justificação estratégica elaborada por projeto.

5.Conclusão e trabalho futuro

Neste último capítulo apresentam-se as principais conclusões baseadas no trabalho de investigação e na elaboração do caso prático para demonstrar a solução para o problema identificado durante a investigação. São também abordados trabalhos futuros na perspetiva de correção das falhas encontradas e melhoria da solução.

5.1. Análise do caso prático

Seguir o CobiT 5 para perceber a capacidade dos processos relacionados com as TIC, revelou ser um prazeroso exercício de reconhecimento e vislumbre. A utilização deste para aferir/auditar a capacidade de governação e gestão das TIC, parece ser aquele professor que tudo sabe, e até ensina sobre tudo aquilo que se pensa saber.

O altruísmo que o CobiT 5 revela ao apontar as normas no qual se baseia como por ex. a ISO/IEC 27000 ou mesmo outras *frameworks* como a ITIL, são indicadores da abrangência, alcance e profundidade que este possui.

Das sete fases de melhoria contínua que carateriza a utilização do CobiT no seu processo de apoio à criação de valor com a otimização de recursos e risco, só foi possível no tempo útil desta investigação, chegar à fase 4. Desta situação tiram-se logo conclusões sobre a morosidade de cada interação do programa, e que só por si é um risco à sua credibilidade e sucesso. O Cobit 5 identifica como fundamental a mitigação de alguns riscos, como por exemplo, o necessário apoio do executivo sem o qual todos os trabalhos poderão ser infrutíferos devido às questões de mudança, sempre muito complicadas, no âmbito cultural da administração pública.

Este trabalho mostra, através do programa de implementação baseado no guia de implementação do CobiT 5 [4], os primeiros passos para a criação de uma EGTIC para a administração pública local. Este resultado, que embora possa parecer "minimalista" era esperado atendendo:

- "*One of the common reasons why some GEIT implementations fail is that they are not initiated and then managed properly as programmes to ensure that benefits are realised. GEIT programmes need to be sponsored by executive management, be properly scoped, and define objectives that are attainable so that the enterprise can absorb the pace of change as planned. Programme management is therefore addressed as an integral part of the implementation life cycle.*" [4]
- "*The implementation programme will be closed when the process for focusing on IT-related priorities and governance improvement is generating a measurable benefit and has become embedded in ongoing business activity*." [4]

Analisando os resultados obtidos do uso do CobiT 5 conforme visto em todo o capítulo 4 e onde na secção 4.3.4 é selecionado um processo para capacitar, conclui-se que este não diz diretamente respeito a questões de segurança ou garantia da informação, deixando aqui à primeira vista comprometido o objetivo proposto nesta

dissertação. No entanto, conforme se observa no parágrafo anterior, este é um processo contínuo e o programa de implementação só termina quando este fizer parte da cultura da organização, podendo assim gerar resultados mensuráveis.

Para ajudar nas conclusões é necessário analisar o CobiT 5 na perspetiva da segurança e garantia da informação, conseguindo-se identificar uma série de atividades relevantes e que remetem diretamente para a gestão de risco, segurança da informação e garantia dos dados:

- **Classificação dos dados**, porque é importante classificar todo o tipo de dados sensíveis e o fluxo que estes possuem dentro do sistema como um todo. Neste ponto também se julga importante que o município tenha forma de conhecer o ciclo de vida de todos os seus ativos de informação:
    - APO01.06 - Definir a propriedade da informação (dados) e sistemas;
    - APO03.02 - Definir a arquitetura de referência;
- **Monitorizar e avaliar os fornecedores quanto à conformidade** com políticas existentes assegurando as condições de segurança da informação e cumprimento dos contratos e SLA, garantindo que os incidentes de segurança e problemas são geridos da forma correta:
    - APO10.05 - Monitorizar o desempenho e conformidade dos fornecedores;
- É considerado essencial que seja usado uma **metodologia baseada na análise de risco** para priorizar as respostas às falhas de segurança de uma forma rápida, reduzindo assim ao mínimo ou mesmo eliminar o impacto no município ou partes interessadas:
    - APO12.06 - Responder ao risco;
- A **existência de um SGSI** fornece uma perspetiva coordenada de segurança da informação para o município, pois permite implementar controlos de uma forma coerente. A segurança da informação é obtida através da implementação de um conjunto adequado de controlos, incluindo políticas, processos, procedimentos e estruturas organizacionais. Estes controles precisam ser estabelecidos, implementados, monitorizados, revistos e melhorados, sempre que necessário, para garantir que os objetivos de segurança e de negócios específicas do município possam ser alcançados:
    - APO13.01 - Estabelecer e manter um SGSI;
- Qualquer organização deve lutar de forma eficaz contra a **manipulação maliciosa de dados sensíveis**. Existem basicamente duas abordagens para o fazer, i) soluções de rede ii) soluções orientadas ao utilizador:
    - DSS05.01 - Proteger contra o *malware*;

    - DSS05.02 - Gerir a rede e a segurança das conexões;
    - DSS05.03 - Gerir a segurança dos *endpoints* (terminais);
    - DSS05.04 - Gerir a identidade dos utilizadores e os acessos lógicos;
    - DSS05.05 - Gerir o acesso físico a ativos TIC;
    - DSS05.06 - Gerir documentos sensíveis e dispositivos de saída;
    - DSS05.07 - Monitorizar a infraestrutura para eventos relacionados com a segurança;
- A **monitorização de todo o processo ou controlos** implementados permite garantir o cumprimento dos requisitos internos e externos estabelecidos. Dentro do ciclo de vida continuo e de melhoramento do CobiT e nos resultados destas monitorizações, será possível garantir ajustes e melhorias os processos:
- MEA01.03 - Recolher e processar dados de desempenho e conformidade;
- MEA02.02 - Rever a eficácia de controlos de processos de negócio;
- MEA03.02 - Otimizar a resposta a necessidades externas.

No caso exemplificado na secção 4.3 a opção de capacitação recaiu sobre todo o processo DSS02- Gerir pedidos de serviço e incidentes, Anexo 3 - DSS02 - Gerir pedidos de serviço e incidentes, que se encontra, no fim desta investigação, em fase de implementação, não sendo assim possível no tempo útil aferir objetivamente os benefícios espectáveis.

Assim, as conclusões aqui expressas são a ilação sobre os resultados esperados com a implementação do processo em relação ao objetivo desta dissertação, e de acordo com a justificação estratégica elaborada. Também é percetível que não é possível apresentar uma análise concreta sobre os ganhos obtidos com a capacitação do processo, pois para isso será necessário chegar à fase 7 do ciclo de melhoria contínuo.

Analisando o processo DSS02 no Anexo 3 - DSS02 - Gerir pedidos de serviço e incidentes, é possível perceber que a sua capacitação irá melhorar o processamento e disponibilidade da informação. Ter garantia de informação é também ter garantia que esta pode ser processada e disponibilizada de forma segura com o mínimo de tempo de disrupção, o que é capacitado com o DSS02. De seguida, a descrição e o propósito do processo, e sublinhar a ajuda na garantia da informação.

Processo DSS02

Descrição: Fornecer uma resposta atempada e efetiva a pedidos dos utilizadores e resolução de todo o tipo de incidentes. Restaurar a normalidade do serviço; registar

e completar os pedidos do utilizador; e registar, investigar, diagnosticar, escalar e resolver incidentes.

Declaração de Propósito: Alcançar a melhoria na produtividade e minimizar interrupções através de resoluções rápidas a pedidos de utilizador e incidentes.

De notar também que este processo necessita dos *inputs* APO12.06 e DSS05.07, atrás identificados, como relevantes para diretamente gerir o risco e garantir os ativos de informação, pelo que já serão também capacitados nesta primeira iteração do programa de implementação.

Novamente é importante perceber que no processo de governação e capacitação de processos, no ciclo de melhoria contínua, o natural será o de capacitar os priorizados mediante as necessidades objetivas da organização para a **obtenção do valor pretendido**. Concluindo-se aqui que a segurança da informação é salvaguardada ao nível do **risco assumido**, garantindo-se a **otimização dos recursos** com a priorização (pela EGTIC) baseada em justificações estratégicas.

A aplicação de controlos de segurança é também desta forma levada em conta na medida das necessidades identificadas pelas partes interessadas através do processo de governação. Assumindo que a *framework* orienta para as reais necessidades dentro de cada processo capacitado.

Na perspetiva da garantia da informação (*information assurance*) fica demonstrado o foco na estratégia alinhada com a forma holística de ver o risco e a sua mitigação na organização. Com a capacitação orientada por estruturas reconhecidas, é levada em consideração em cada interação a conformidade dos processos (entre si, com outros e com as questões legais). Com a orientação estruturada e seguindo as justificações estratégicas também se garante o estudo da continuidade e processo de recuperação. Na perspetiva da segurança da informação (*information security*), em cada justificação estratégica de novas propostas de projetos, é obrigatório a inclusão das ferramentas e táticas levando também em conta a questão segurança. A própria escolha das ferramentas (antivírus, firewall, IDS…) é efetuada na medida de uma proposta de justificação estratégica que irá assim também garantir a informação com otimização dos recursos.

5.2. Contribuição do trabalho efetuado

Como identificado e explicado na subsecção 2.2.2, a nível nacional existe um plano para a racionalização dos recursos TIC [34], este plano possui um conjunto de tarefas a cumprir por forma a se atingirem os objetivos estipulados e que passam por melhorar o serviço público, com um menor custo. Esta dissertação foca exatamente

essa preocupação, ou seja, conseguir garantir o melhor para o serviço público na administração local, fazendo a otimização do risco e dos recursos.

"No âmbito do presente plano descrevem-se as ações transversais que se consideram fundamentais para mudar a forma como o Estado incorpora as TIC na sua atividade, bem como, para potenciar as TIC enquanto indutoras da modernização." [34] A integração da governação das TIC na governação do município e reconhecer o papel de parceiro de negócio no desenvolvimento de soluções e novas áreas para gerar valor público, apoia a transparência fundamentada no uso de normas e *frameworks* reconhecidos internacionalmente.

Importa salientar a disseminação do conhecimento sobre o que é uma EGTIC e o seu contributo para uma governação pública melhor. Devemos destacar também a importância de nivelar as propostas de capacitação de soluções, sistemas ou processos através do uso de uma justificação estratégica com parâmetros comparáveis, permitindo assim a priorização do investimento.

Em outra vertente, e sendo conhecido que muitas vezes a aferição do estado dos serviços TIC e sistemas de informação existentes nos municípios é feito de forma ad hoc ou com recursos a auditores externos, mostrou-se que a utilização das ferramentas do CobiT 5 para efetuar essa análise de capacidade, é bastante reveladora e eficaz. Abre-se assim uma porta para a primeira fase de implementação da EGTIC, criar o desejo de agir.

"IT governance is needed to ensure that the investments in IT generate value reward and mitigate IT associated risks, avoiding failure. IT is central to organisational success – effective and efficient delivery of services and goods – especially when the IT is designed to bring about change in an organisation. This change process, commonly referred to as "business transformation," is now the prime enabler of new business models both in the private and public sectors." [45]

5.3. Trabalho futuro

No decorrer da investigação e mais concretamente na efetivação dos levantamentos necessários para realizar as tarefas preconizadas em cada fase do ciclo de melhoria contínuo do CobiT 5, foi detetada uma falha relativa à arquitetura empresarial e que deverá em trabalhos futuros ser explorada por forma a se melhorar a contribuição da EGTIC para a garantia da informação e dos TIC como parceira de negócio. A dificuldade no entendimento sobre os serviços prestados no município, bem como, a uniformização dos procedimentos municipais quer a nível local como nacional, são

matérias que merecem ser exploradas por forma a facilitar o encaixe da arquitetura tecnológica e aplicacional ao nível exato do pretendido.

"*From the perspective of the 'relationship economy' the new capabilities and possibilities created by information and communication technology* [12]*are essential for successfully pursuing long-standing relationships with customers, and for employees supporting them. The vast amount of actions and data pertinent to customers, and their relationships, desires and needs, can only be meaningfully and effectively addressed with the help of ICT*." [46]

A exploração da nova área da engenharia empresarial abre portas para a verdadeira modernização administrativa e criação de valor público com os investimentos TIC. Torna-se premente nos dias de hoje a existência de um real conhecimento de todos os atores e papéis no decorrer de todos os processos empresariais, só assim deverá ser possível antecipar falhas, e garantir serviço.

[12] *Information and Communication Technology*

Referências Bibliográficas

De seguida é apresentada toda a bibliografia consultada e usada de forma referenciada ao longo de todo o trabalho.

[1] M. Gerrard, "IT Governance - Key Initiative Overview," 2010. [Online]. Available: http://www.gartner.com/it/initiatives/pdf/KeyInitiativeOverview_ITGovernance.pdf. [Acedido em 20 Fevereiro 2013].

[2] C. Symons, S. Leaver, C. Gliedman e T. DeGennaro, "IT Governance And Risk," Forrester Research, Cambridge, 2010.

[3] P. Weill e e. W. Ross, IT Governance: How Top Performers Manage IT Decision Rights for Superior Results, Harvard Business School Press, 2004.

[4] ISACA, CobiT 5 - Implementation, Rolling Meadows: ISACA, 2012.

[5] National Institute of Standards and Technology, "NISTIR 7298 Revision 2," U.S. Department of Commerce, 2012.

[6] Grecs, "Nova Infosec," 30 Agosto 2011. [Online]. Available: https://www.novainfosec.com/2011/08/30/information-assurance-versus-information-security/. [Acedido em 22 Junho 2013].

[7] R. J. Robles, J.-Y. Park e T.-h. Kim, "Information Security Control Centralization and IT Governance for Enterprises," *International Journal of Multimedia and Ubiquitous Engineering,* Vols. %1 de %2Vol. 3, No. 3, pp. 67-75, Julho, 2008.

[8] ISACA, CobiT 5 - A Business Framework for the Governance and Management of Enterprise IT, Rolling Meadows: ISACA, 2012.

[9] A. Cresswell, G. B. Burke e T. Pardo, *Advancing Return on Investment Analysis for Government IT,* Albany: Center for Technology in Government, University at Albany, 2006, Setembro.

[10] ISACA, "Web - COBIT 5: A Business Framework for the Governance and Management of Enterprise IT," ISACA, 2012. [Online]. Available: http://www.isaca.org/COBIT/Pages/default.aspx. [Acedido em 20 Janeiro 2013].

[11] ITIL, "Official ITIL WebSite," APMG em conjunto com o Cabinet Office do Governo do Reino Unido, [Online]. Available: http://www.itil-officialsite.com/. [Acedido em Janeiro 2013].

[12] APM Group, "ISO/IEC 20000 certification," [Online]. Available: http://www.isoiec20000certification.com/home/home.aspx. [Acedido em Janeiro 2013].

[13] The ISO 27000 Directory, "The ISO 27000 Directory," [Online]. Available: http://www.27000.org/index.htm. [Acedido em Janeiro 2013].

[14] K. V. Wal, J. Lainhart e P. Tessin, "A COBIT 5 Overview," em *2012 ISACA Webinar Program*, 2012.

[15] ITIL Survivel, "ITIL Survivel," Abril 2011. [Online]. Available: http://www.itilsurvival.com/cctaitil.html. [Acedido em Abril 2011].

[16] M. Andenmatten, "Eine Roadmap zu ITIL Lite," 19 Novembro 2011. [Online]. Available: http://blog.itil.org/2011/11/cobit/eine-roadmap-zu-itil-lite/. [Acedido em 16 Fevereiro 2014].

[17] A. Cartlidge, A. Hanna, C. Rudd, I. Macfarlane, J. Windebank e S. Rance, An Introductory Overview of ITIL® V3, The UK Chapter of the itSMF, 2007.

[18] Wikipedia, "Information Technology Infrastructure Library," [Online]. Available: http://en.wikipedia.org/wiki/Information_Technology_Infrastructure_Library. [Acedido em Janeiro 2013].

[19] Wikipedia, "Wikipedia - ISO 20000," 23 Julho 2013. [Online]. Available: http://pt.wikipedia.org/wiki/ISO_20000. [Acedido em 18 Outubro 2013].

[20] Pink Elephant, "Pink Elephant The IT Management Experts - ISO/UEC 20000 Foundation," [Online]. Available: http://www.pinkelephant.com/Products/Education/Foundation/ISE.htm?LangType=7177. [Acedido em 23 Outubro 2013].

[21] The ISO 27000 Directory, "A Short History of the ISO 27000 Standards," 2007. [Online]. Available: http://www.27000.org/thepast.htm. [Acedido em Julho 2013].

[22] S. Higgins, "Information Security Management: THE ISO 27000 (ISO 27K) SERIES - See more at: http://www.dcc.ac.uk/resources/briefing-papers/standards-watch-papers/information-security-management-iso-27000-iso-27k-s#sthash.eL5WO29p.dpuf," 19 Março 2009.

[23] Wikipedia, "King Report on Corporate Governance," 28 Outubro 2013. [Online]. Available: http://en.wikipedia.org/wiki/King_Report_on_Corporate_Governance. [Acedido em 08 Novembro 2013].

[24] R. Butler e M. J. Butler, "Beyond King III: Assigning accountability for IT governance in South African enterprises," *South African Journal of Business Management,* vol. 3, p. 41, 2010.

[25] J. Terblanche, *An information technology governance framework for the public sector,* Stellenbosch: Master Thesis - University of Stellenbosch, Dezembro de 2011.

[26] M. R. A. Cedraz, "RELATÓRIO DE LEVANTAMENTO - Governança de tecnologia da informação na Administração Pública Federal - TC nº 000.390/2010-0 Fiscalis nº: 45/2010," TCU, Brasilia, 2010.

[27] T. d. C. d. União, "RELATÓRIO DE LEVANTAMENTO - TC 007.887/2012-4.," TCU, Brasilia, 2012.

[28] A. -. Municipality, "Information Technology - Austin, Texas," [Online]. Available: http://www.austintexas.gov/department/information-technology/about. [Acedido em 15 Setembro 2013].

[29] R. Garza, S. Hensley e S. Elkins, "City of Austin - Information Technology Strategy 2012-2017," Austin, 2012.

[30] R. J. H. Varn, "Information Techonology Strategic Plan FY10-FY13," City of San Antonio, San Antonio, 2010.

[31] MN.IT SERVICES, "IT GOVERNANCE FRAMEWORK," Esdado do Minnesota, Saint Paul, Junho de 2012.

[32] City of Ottawa- Information Technology Services, "Technology Roadmap 2013-2016," City of Ottawa, Ottawa, Novembro de 2012.

[33] A. Baxter, S. Cox e D. Snowdon, "Brighton & Hove City Council ICT Strategy 2011-2016," Brighton & Hove City Council , Brighton & Hove, 2011.

[34] Gupo de Projeto para as Tecnologias de Informação e Comunicação, "Plano global estratégico de racionalização e redução de custos nas TIC, na Administração Pública," Governo Português, Lisboa, 2011.

[35] A. p. a. P. e. d. d. S. d. informação, *13ª tomada de posição do Grupo de Alto Nível,* Lisboa, 2012.

[36] D. A. d. S. Nunes, *Improving the IT Strategic Plan for the Public Administration in Portugal,* Lisboa: Instituto Superior Técnico, 2013.

[37] M. Lavado, *Maturidade da Governação e Gestão de TI em Portugal - Inquérito Nacional,* Lisboa: itSMF Portugal, 2011.

[38] Municipio de Portimão, *Diário da Republica, 2ª Série - N.º185 - Despacho n.º 12266/2013,* Lisboa: Casa da Moeda, 25 de Setembro de 2013.

[39] M. d. Portimão, "Despacho n.º 4176/2013," *Diário da República Portuguesa,* pp. 10062 - 10083, 20 Março 2013.

[40] BDO, "Revisão de Controlos IT - Carta de Recomendações," Portimão, Fevereiro de 2013.

[41] E. Kaselowski, *Mitigating Risk Through Effective Information Technology Operations in Local Governments - Towards a Best Practice,* Nelson Mandela Metropolitan University, 2008.

[42] Município de Portimão, "Orçamento da receita da despesa de 2013 e grandes opções do plano 2013-2016," Portimão, 2013.

[43] J. Tribolet, "Que aprendizagens retira dessa área que possam ser úteis para Portugal?," 2013. [Online]. Available: http://www.youtube.com/watch?v=Pb2ofiwsHyY. [Acedido em 15 Setembro 2013].

[44] Governo Poruguês, "Resolução do Conselho de Ministros n.º 112/2012," *Diário da República,* pp. 7307-7319, 31 Dezembro 2012.

[45] D. Radovanović, M. Šarac e S. Adamović, "Necessity of IT Service Management and IT Governance," em *MIPRO 2011*, Opatija, Croatia, 2011.

[46] J. . L. Dietz e J. . A. Hoogervorst, "The discipline of enterprise engineering," *Int. J. Organisational Design and Engineering,* Vols. %1 de %2Vol. 3, No. 1, nº enterprise engineering, pp. 86-114, 2013.

[47] K. Peffers, T. Tuunanen, M. Rothenberger e S. Chatterjee, "A Design Science Research Methodology for Information Systems Research," *Journal of Management Information Systems,* vol. 24, pp. 45-78, 2007/2008.

[48] S. M. A. Correia e A. Lucas, *Factores Críticos de Sucesso da Governança dos SI/TI,* Lisboa: CAPSI2009, 2009.

[49] ITpreneurs Nederland B.V., ISO/IEC 20000 Practitioner - Student HandBook, ITpreneurs, 2012.